

https://dspace.org/

To What Extent Have Cyber Sabotage and Cyber Espionage Undermined the National Security of South Africa, Kenya and Ethiopia, 2016- 22

Kinnes, Shaun

2024

University of the Witwatersrand, Johannesburg

https://hdl.handle.net/10539/45709

Kinnes, Shaun . (2024). To What Extent Have Cyber Sabotage and Cyber Espionage Undermined the National Security of South Africa, Kenya and Ethiopia, 2016- 22 [Master`s dissertation, University of the Witwatersrand, Johannesburg]. WIReDSpace. https://hdl.handle.net/10539/45709

Downloaded from a DSpace repository. https://dspace.org/

2/15/2024

To What Extent Have Cyber Sabotage and Cyber Espionage Undermined the National Security of South Africa, Kenya and Ethiopia, 2016-22

DR Sizwe Mpofu-Walsh

Shaun Kinnes
STUDENT NO:2137261

Declaration:

I, the undersigned, Shaun Kinnes, do hereby make an oath that this thesis is my own unaided work. It is submitted for the degree of Master of Arts at the University of the Witwatersrand, Johannesburg. It has not been submitted for any other degree before, or for examination at any other university.

Signature of Candidate: *S.C Kinnes*

15 February 2024

Table of Contents:

Part I
Introduction and Background……. Page 5-9
Case Selection……Page 9-11
Research Question……. Page 11
Hypothesis……. Page 11
Methodology……Page 11-13
Research Problem and Contribution to Literature…. Page 13-15

Part II
Literature Review……Page 16-24
Theory……. Page 25-34

Part III: Case Studies
South Africa……. Page 34-43
Ethiopia……Page 44-48
Kenya……. Page 49-53
Making Sense of it All……. Page 54-60
Conclusion……. Page 60-67
Bibliography……Page 68-71

Acknowledgements:

Though the journey was hard and the road tough I wish to thank all those who helped carry me through my master's journey.

I wish to thank the South African Institute of International Affairs and the Konrad Adenauer Stiftung for the generous financial and intellectual support provided to me that contributed greatly to the completion of my master's degree.

To my supervisor Dr Sizwe Mpofu-Walsh, I wish to express my endless gratitude for words of wisdom, informative critique and mentorship that assisted me in captaining the ship toward eventual submission of my research.

I wish to also thank my family and friends for their emotional support during this challenging journey. So, to them, I say thank you for all the late-night talks and morning coffees. To my darling mother and sister especially know that both of you have been my rock.

Furthermore, I thank God for giving me the strength and wisdom to pursue such as daunting journey. To an extent, I must also pay homage to myself for being consistent and steadfast in my decision to undertake and complete this research as was no easy task.

Key Terms:

- Cyber Offence
- Cyber Defence
- National Security
- SADC- Southern African Development Community
- Cyber Sabotage
- Cyber Espionage
- Cyber Security
- Cyber domain
- Cyber army
- Cyberspace
- GERD- Grand Ethiopian Renaissance Dam

If The River's Level Drops, Let All the Pharaoh's Soldiers Hurry and Return Only After the Liberation of The Nile-Restricting Its Flow. To Prepare the Ethiopian People for The Wrath of The Pharaoh's. — [Samme-Nlar 2022,174]

Introduction and Background: (Part: I)

The world is changing, emerging technologies now form part of the daily lives and functions of every individual, bureaucracy and business. With the rise of technologies such as artificial intelligence, quantum computers and a tech-savvy youth, this brought with it tremendous opportunity but also newfound challenges. In short, disruption needs planning. As the leapfrogging of technology will bring with it new advantages, such as an improvement in innovation, job creation and increased revenue, it will also bring with it disadvantages such as cybercrime, cyber sabotage and cyber espionage, which states more especially in the African continent must be prepared to grapple with. Fatima Roumate highlights this perfectly as she draws upon how the malicious use of technology creates new challenges for states as the original actors in International Relations, considering the rise of new notions such as artificial diplomacy, data sovereignty, cyber security and cyberwarfare (Roumate 2021,1-4).

National security strategies must be prepared to deal with unconventional challenges posed by the emergence of the technological revolution. National security, which was originally conceptualised as protection against military attacks in the digital age the world now finds itself in; national security must be reconfigured to include non-military dimensions such as cyber security. Hence, the call is for cyber security to be added as an additional pillar alongside conventional national security pillars. Melvin Kranzberg's law of technology denotes that 'technology is neither good nor bad; nor is it neutral (Kranzberg 1964,578-580). Ultimately national cyber security strategies are of utmost importance, as when used for good technology is an iron blade in advancing societal development, but when utilised for bad, technology is an existential threat to the survival of the state and humanity.

Ultimately, it is in the national interest of states to secure the cyber realm. It is for this reason that Brian Njama Kiboi calls for the broadening and deepening of national

security objectives, as this should ideally extend beyond the military sector and include the cyber realm (Kiboi 2015, 11). Melvyn P. Leffler also elaborates on how national security encompasses the decisions and actions vital to safeguard the homeland against external threats (Leffler 1990,143).

States face cyber risks, including ransomware attacks, malware, cyberterrorism and network application anomalies. Laurent Colerier and Jose Araujo define these as cyber incidents which pose risk to the national security of states while defining ransomware as the encryption of data as a means of extorting compensation for the return of data files; this can also be referred to as cyber hostage-taking incidents; while malware is described as software that without the permission of a host alters data via delivering viruses to data systems and critical infrastructure. Network and application anomalies, such as tunnelling attack network traffic and communications between servers (Colerier and Araujo 2023,11). Brian Njama Kiboi defines cyberterrorism as the act of terrorist organisations using cyber means to terrorist acts against public targets as a means of making public statements or aiming to achieve political objectives (Kiboi 2015,48).

It is also worth noting that within the cyber realm concepts such as ‘cyber offence’ and ‘cyber defence’ are two key terms that describe the security complex of the cyber realm. PC Duvenage and SH Von Solms define cyber defence as defensive systems that safeguard data and critical systems from hacking or data being stolen by adversaries, while also generating information about adversaries; cyber offence is referred to as offensive counterintelligence, whereby the objective is to eliminate an adversary’s advances via measures ranging from cyber deception to cyber manipulation to the neutralisation of adversarial intelligence activities and systems (Duvenage and Von Solms 2015,46-47).

One must also note that cyber offence and cyber defence can be classified into two sub camps. Within the cyber offence realm notions such as passive and active offence come into play. Passive offence entails showing the enemy what the protecting system wants it to see also known as selective exposure, while active offence is covert action in tracking down an adversary; passive defence entails denying an enemy access to critical systems, via security measures and systems, active defence entails the collection of information of an enemy trying to breach a system as a means of

determining who is behind the breach, and passing the information onto offensive security personal for action (Duvenage and Solms 2015, 49-50). Such measures are exceptionally necessary in safeguarding a state's cyberspace.

The cyberspace like global issues such as climate change, global financial crisis and war is an issue that spans beyond control of the nation-state. It is an emerging transnational issue that requires the development of norms and practices if states and other entities are to peacefully exist within the cyber domain. States by virtue are also compelled to cooperate on issues that are classified as existential threats to their citizens and society as a whole. Ultimately, states, civil society, and regional and international organisations are compelled to work closely with each other as a means of fueling information sharing, and cyber development research including international and regional conventions on cyberspace.

Nnenna Ifeanyi-Ajufo draws upon how the promotion of security and stability within the cyber environment can be enhanced via adopting appropriate policies and building cooperative measures which can contribute to appropriate cyber governance (Ajufo 2023,3). Two major African continental policies developed on the African continent include the 'Malabo Agreement' and 'AU Declaration on Internet Governance', with the Malabo Agreement at present, entailing the main objective of developing common cyber norms and protection while spearheading information sharing between signatories. The Malabo Agreement is a key milestone in ensuring the African continent's commitment to increased cyber security awareness and information sharing. Once operational all 55 AU member states are expected to have domestic legislation around cyber security, information sharing and cyber systems. It is vastly disappointing that in the present only 15 African states have ratified the Malabo Agreement. the AU Declaration within the legislation has adopted cyber security as a flagship project of the African Union Agenda 2063 (Ajufo 2023,4).

Along with this, actors should essentially be pooling knowledge. Cyber development is mainly fueled by the private sector and military industries including academia. Karen Allen highlights the notion of 'techplomacy', a discipline of diplomacy that acknowledges the power and influence of big tech corporations within the new world order (Allen 2023,1). Hence, the private sector should be working closely with the state as a means of safeguarding national cybersecurity. Within the South African

context, private sector cyber security is exceptionally resilient within South African banks in particular having gold standard cyber security, most cyber-attacks that currently plague the country occur within the public sector, notable victims include Transnet, the South African Social Security Agency and the City of Johannesburg. Showing that there is vast room available for cooperation between private and public sectors of society as a means of bolstering cyber security.

Cyber espionage means the usage of digital technology to spy on an adversary state, and cyber sabotage means the usage of digital technology as a means of causing damage to critical cyber systems of an adversary state (Allen, La Lime and Nlar 2022, 2-3). These are the factors at play that must be seen as imperative for national security and intelligence communities to safeguard and mitigate against.

Notable cyber incidents of cyber espionage and cyber sabotage on the African continent have emanated from outside the African continent- but also from within the African continent. In 2018 Richard Gowan, Mathieu Duchatel and Lafont Rapnouil revealed how it was discovered that the newly built African Union Headquarters sponsored by the Chinese state had been bugged, it had been revealed that for five years carefully concealed listening devices had been hidden in the walls of the AU, whereby Chinese actors could listen in on intelligence and convert meetings between African policymakers and heads of state and relay information back to actors within the Chinese state (Gowan, Duchatel and Rapnouil 2020,14).

In 2019 after a strain in diplomat relations between South Africa and Rwanda, it was uncovered that President Cyril Ramaphosa's cell phone calls were being monitored carefully by Israeli-designed Pegasus software; a covert spying software that essentially turns one's electronic device into a spying device where one can be listened to and tracked. Carien du Plessis argues how this cyber device was traced back to Rwanda, which ultimately further strained relations between Pretoria and Kigali (du Plessis 2021,2)

Cybercrime is also a major issue on the African continent, most especially since the emergence of the COVID-19 pandemic, where life as we knew it moved to a more online and electronic means of engaging. Tim Hall and Ulrike Ziemer draw upon how cybercrime is essentially placeless and can be carried out from anywhere in the world, with Nigeria and Ghana ranked as the most prominent African states affected by

cybercrime (Hall and Ziemer 2023,8). Cybercrimes are committed by a plethora of actors given its relative ease, Tamara Hendriksen highlights how if cybercrime was an economy, it would be the world's third-largest economy after the United States of America and China (Hendriksen 2022,4).

States, illicit criminal actors and tech-smart individuals are all potential cyber criminals. North Korea for one routinely employs cyber technologies as a means of stealing financial assets to finance the North Korean regime. Organised crime cartels have added cyber to their list of illicit activities as a means of increasing illicit financial flows, employing cybercrimes such as phishing and business email compromise. Illicit financial flows drawn from cybercrimes can be linked to Achille Mbembe's terming of the 'raw economy', whereby he argues that illicit financial flows form part of a shadow economy, where money circulates the global financial system outside of legal reckoning as the logic of extraction underpins the raw economy (Mbembe 2012, 27).

Inequality, unemployment and a tech-savvy youth may also lead to conditions ripe for the emergence of cybercriminals. Also dubbed lone wolf attackers, where individuals earn a living through engaging in cybercrime. Alternatively, just as private military contractors such as the Russian Wagner Group or South African Dyck Industries offer their services to the highest bidder while in turn also throwing in the notion of plausible deniability; cyber-criminal groups such as Egyptian based 'Cyber Horus Group' and Nigerian-based 'Black Axe', routinely outsource their cyber skills to the highest bidder at a cost which often include attacks against states.

As a result of this phenomenon intelligence communities and national security operatives must be cognisant of the fact that just as they employ cyber technology to safeguard and counter cyber criminals, so do cyber criminals employ technology to attack the state. Fabio Cristiano, Xymena Kurowska and Dennis Broeder express this same point as they draw upon how military and intelligence communities must understand the notion that technology can both produce security and be an object of security concern (Cristiano, Kurowska and Broeder 2024,21).

Case Selection

For this research, South Africa, Kenya, and Ethiopia will be used as case studies. As a result of cyber innovation and development only taking place within certain pockets on the African continent; one can draw upon how cyber security cannot be equally measured. Africa is also a vastly diverse continent, encompassing 54 states: with different security complexities, cultures and traditions.

Ultimately, South Africa, Ethiopia and Kenya were chosen based on these states largely seen as powerhouses on the African continent. All the selected case study states have developed national cyber security strategies and have also achieved notable advancements in their cyber innovation and development programmes. These states have also encountered a vast array of cyber threats, that have to a various extent undermined both their national credibility and security. Cyber responses to acts of cyber espionage and cyber sabotage also varied in each case; with certain cases showing more cyber resilience than other counterparts. South Africa, Kenya, and Ethiopia are also classified as African states that are amongst the world's at-risk states in terms of cybercrimes such as ransomware.

Ultimately, the acts of cyber incidents that will be investigated will include the 2021 ransomware incident on Transnet (South Africa), the 2021 malware attack of 33 000 Ethiopian service systems (Ethiopia), and the 2019-2022 phishing incident on Kenyan ministries of finance, foreign affairs and office of the president (Kenya). All these cyber incidents that plagued these states had far-reaching economic, political and security ramifications and in the case of South Africa, the cyber incident impacted negatively not only on the South African state but the broader African region as well.

Research Question:

The main question this research aims to understand is 'To what extent have cyber sabotage and cyber espionage undermined the national security of South Africa, Kenya and Ethiopia, 2016-2022'. With key sub-questions such as what the economic ramifications of each cyber incident to the state were and how these cyber incidents bring about further instability.

Hypothesis:

The hypothesis that will guide the study will entail the following: In periods of internal instability or geo-political conflicts, South Africa, Ethiopia and Kenya's cyber resilience decreases while being unable to respond effectively to cyber incidents and even deviating from cyber security strategies.

Methodology:

For this research project, this study will be qualitative; employing qualitative methods such as the use of process tracing and comparative case study analysis, as this study will make use of three case study African states; which include South Africa, Ethiopia and Kenya.

Responses to cyber incidents as well as similarities and differences between each cyber incident and response will be investigated. Delwyn Goodrick argues that the entire purpose of a comparative case study analysis research project is aimed at researching two or more cases and producing a more generalised knowledge upon crucial questions, including why particular responses or programmes fail or succeed (Goodrick 2014,1-2). Hence, how cyber incidents of cyber sabotage and cyber espionage affected the national security of South Africa, Kenya and Ethiopia will be investigated, including how each response differed and where there was similarity in response or outcome. Investigating similarities and differences in the outcome of cases is exceptionally important within the context of a comparative case study analysis project. Delwyn Goodrick draws upon how comparative case study analysis performs the important task of emphasising comparison within and across contexts involving the analysis of the synthesis of similarities; differences and patterns across two or more cases that share a common focus or goal (Goodrick 2014,1).

As the research aims to identify certain similarities and differences between cyber incidents, it is then that variables that can be associated with certain outcomes between and within cases will also come to light. Authors Claudia Pahl-Wostl, Xavier Basurto and Sergio Villamayor Tomas highlight how as part of a comparative case study analysis; a case-oriented analysis is also critical as it aims to identify variables that are associated with outcomes within certain cases, and environments and involving certain actors (Wostl, Basurto and Tomas 2021,288).

Process tracing will also be utilised within the context of this research. As comparative analysis aims to investigate similarities and differences between cases, the function of process tracing is aimed at looking at the sequence of events that lead to an outcome. Cyber security or rather cyber insecurity has important ramifications for national security, trade, finance and even healthcare; ultimately, consequences of cyber insecurity are connected so to be effective solutions must be interconnected. Process tracing does a good job of mapping the sequence of interconnections between cause and outcome, which is of vital importance in the context of this study.

David Collier himself mentions how process tracing provides deeper attention to the sequence of independent, dependent and intervening variables; in a similar light process tracing can make decisive contributions to diverse research objectives, which include; identifying political, social and novel phenomena while systematically describing each, evaluating or discovering existing hypotheses and assessing new casual claims, providing an alternative means-compared to conventional regression analysis and inference based on statistical models of addressing challenging problems such as reciprocal causation, spuriousness and selection bias (Collier 2011,823-825). Process tracing is also a simple tool for giving a well-articulated, factually sound breakdown of a complex event or phenomenon.

Research Problem and Contribution to Literature:

Cyber security is an emerging challenge for the national security of South Africa, Kenya, Ethiopia and all states around the globe. At present, Kenya, South Africa and Ethiopia are considered some of the worst affected states by cyber-attacks in the world. The total cost of cyber espionage and sabotage amounts to around 5 billion USD to the South African economy (Wolf, Cloete and Hofmeyer 2022,15-22).

Whatever the motivation or location of cyber hackers, these attacks have direct security, financial and social ramifications for South Africa, Ethiopia and Kenya. Hence, cyber-attacks have direct impacts not only on the economies of these countries but impact their national security aims and objectives as well. Ultimately, cyber security has become a major issue for the African continent, across both private and public sectors and needs to be adequately understood in relation to a state's national security.

It is therefore clear that, when considering the proliferation of cyber-attacks on the African continent but especially in South Africa, Ethiopia and Kenya; the states' sensitivity to such attacks; and the lack of well-developed cyber security policy from each state, a thorough review is necessary of where each state stands concerning cyber security, and the importance of cyber security to the national security frameworks of South Africa, Kenya and Ethiopia. As such, this analysis aims to provide an exploratory study on cyber security as an emerging issue for Kenya, South African and Ethiopian national security.

Cyber espionage and cyber sabotage will be reflected upon as key aspects threatening the national security of African states such as Ethiopia, Kenya, and South Africa between the period 2016-2022. Cyber espionage is defined as the unauthorised use of computer networks and other resources to access or transfer secret, classified, or sensitive information from state servers to unauthorized parties (Suri 2022, 98-102). Cyber sabotage on the other hand is the deliberate and unauthorised alteration of cyber systems i.e. computer networks, and digital grids.

Cyber security is extremely relevant to the study of International Relations as it is a rapidly changing phenomenon vital to the interest of states, regional and international bodies and private sector companies alike. As a means to safeguard against acts of cyber espionage and sabotage; Ethiopia, South Africa and Kenya must adopt national security mechanisms to safeguard national infrastructure and sensitive data systems.

The proliferation of cyber technology has created new vulnerabilities such as cyber espionage and cyber sabotage within the cyber domain, that may be employed to undermine a state's national security. Global North states leverage technology not only for its economic value but also for its strategic value in the sense that cyber tech can be employed to either spy on other states or undermine the stability of rival states.

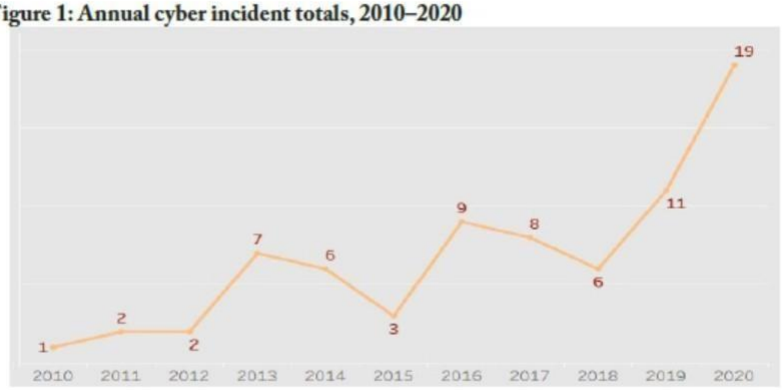
African states employ cyber technology as a means to capitalise upon its benefits, such as using drones to deliver medications to rural areas, employing fintech as a means to drive greater financial inclusion and agri-tech to foster greater food systems. The more technology is employed and relied upon, the greater vulnerabilities African states may face as this leaves them vulnerable to acts of cyber espionage and cyber sabotage by either rival states or non-state actors. This is especially concerning given that many African states have not adopted or developed technologies that afford them the ability to either counter or mitigate the effects of cyber-attacks which range between cyber sabotage and cyber espionage.

According to Deny Reva, since February 2020, when the COVID-19 pandemic forced far more people to adopt increased technologies, cyber security incidents have increased by 400% (Reva 2020,10). Figure 1 shows precisely this as a nearly double figure increase in cyber incidents took place given the rapid move to technology adaptation. Hence, if African states are to seek more cyber tech as a means to drive development, African governments must beef up cyber security within their national security objectives. The protection of confidentiality, integrity and availability of computer data and systems against cyber-attacks is an essential and critical responsibility for all governments. Cyber security should then be a key cornerstone of national security, in the increasingly technologically savvy world that states exist within today. Cybercrimes for one is an act of cyber sabotage, according to Anirudh Suriif; if cybercrime was an economy, it would be the third largest economy globally behind the United States and China (Suri 2022, 212-217). As a result of acts of cyber sabotage being an extremely low-risk; high-reward venture, it is only through the development of a strong cyber security framework that such acts can be either mitigated against or adapted to.

Annual frequency of cyber incidents

As seen in Figure 1, the data revealed annual increases in cyber incidents for most (but not all) of the years studied, with a particularly sharp annual increase from 2019 (11 incidents) to 2020 (19 incidents).

Figure 1: Annual cyber incident totals, 2010–2020



Incident type

Figures 2 to 4 present the classification of the 74 cyber incidents according to incident type, in three periods: 2010-2015, 2016-2018, and 2019-2020. All the cyber incidents are represented by the actual title used in media reports.

Figure Sourced From: African Journal of Information and Communication. The Cyber Threat Landscape (Pieterse 2021,7).

The proposed structure of this research report will be structured as follows: Part one will include an introduction and background to the notion of cyber security. Key pillars such as methodology, case selection, research question and problem will all be elaborated upon. Part two of the research report will include a literature review and examination of key theories relevant to the study being undertaken. Part three of the research report will entail case studies and a conclusion.

Literature Review: (Part: II)

The structure of the literature review aims to identify common debates within the cyber realm and which gaps in the literature this research aims to fill, as a means of adding new literature to this crucial topic.

Common arguments surrounding cyber security on the African continent generally highlight how Africa is lagging within this realm, as a result of not producing cyber-security systems or not having access to the necessary technology transfer agreements as a means of beefing up national cyber security. As one engages the technological landscape on the African continent, it is worthwhile to note that African states generally do not wish to employ technology as a means of driving cyberwarfare against their fellow African counterparts. Instead, technology is viewed as an instrument capable of improving the daily lives of African peoples on the continent and acting as a solution part of overcoming daily struggles.

For one as a means of driving more inclusivity in the financial system African technology entrepreneurs utilise fin-tech technologies as a means of fostering an easier means of undertaking financial transactions. Certain health departments such as those in Rwanda utilise drone technology to deliver medicines to hard-to-reach rural villages. Various African states such as Kenya have rolled out E-citizen services where citizens can apply for passports and identity documents which is aimed at decreasing queues and waiting times, as in previous times citizens had to visit local home affairs ministry offices to access these services. As Ndeapo Wolf, Deon Cloete, and Jan Hofmeyer argue Africa is entering a new ‘digital lifeworld’ for which the ground rules are not yet clearly defined (Wolf, Cloete and Hofmeyer 2022,4).

Threats and Unintended Consequences of Increased Adoption of Technology:

Yes, while these all seem like convenient and even ground-breaking developments, these advancements bring with them unintended consequences. Fin-tech systems, drone technology, energy grids, and E-citizen systems all rely upon computer networks to function effectively. If these systems are compromised via a cyber incident this puts at risk the information and critical system infrastructure of countless individuals, institutional systems and business systems. Timothy M. Mckenzie highlights this factor perfectly as he draws upon how for as long as any state relies upon computer networks as a means of driving military and economic functions,

military and economic security are at risk within the cyber domain (Mckenzie 2017,6). African states must then recognise that with the need to participate within the cyber domain and leverage its benefits, the rate at which they safeguard and implement their national cyber security policies and strategies must keep up with cyber developments as a means of safeguarding and securing such critical infrastructures. Mzukisi Qobo and Mjumo Mzyece add to this point as they argue how cyber institutions of a state underlie state stability, security and development (Qobo and Mzyece 2023,31). As African states seek to adopt increased technology to drive development and integration, this is precisely when policies and networks need to also be implemented to safeguard the increased adoption of technology. Securitisation theory is then relevant within this context, as using the South African case presented within this research- the increased adoption of maritime processing technology to speed up the rate of cargo processing meant that in the event of a cyber incident, this would essentially cripple the cargo processing ability of Transnet. No securitisation policy was implemented leaving the institution naked and vulnerable to cyber incidents such as ransomware and malware attacks.

The question that must be interrogated here is, with Africa becoming a greater participant within the cyber domain, what cyber security strategies, legislation and national security objectives; should they be pursuing as a means of remaining cyber resilient to acts of cyber sabotage or cyber espionage? This is precisely the gap this research aims to fill.

African Solutions to African Cyber Security Needs:

As with any new groundbreaking research or invention, it is understood that knowledge is power; and a means by which agents or in this case- states may translate their agency into influence, to be at the table and not on the menu. Africa is lagging in the development of home-grown cyber technologies; this is a major threat to both national cyber security and Africa's ability to meaningfully participate within the cyber domain. Kevin Hall and Dawie Botha draw upon how there is a huge need for capacity building, which is understood to be the investing in human, institutional and critical infrastructure capacity, to craft stable and secure societies including institutions (Hall and Botha 2010,2).

If African countries simply outsource their needs to cyber consultants or foreign powers, they effectively negate their priority as a state of being the main provider of security to its citizens. Mancha Johannes Sekgololo, argues that African states should bolster production and investment in the cyber realm to avoid adopting the perceptions and technologies of others; as reliance on imported technologies and systems drastically weakens cyber security and national security and instead creates vulnerability to cyber incidents, as foreign states may build backdoors into their systems for cyber espionage purposes (Sekgololo 2021,34).

Former minister of the South African State Security Agency Mr David Mahlobo at the 2015 Cyber Security Symposium hosted by the State Security Agency, uttered that 'We need to be building more partnerships if we are to succeed, our capacity to respond is dependent on systems and human capital development. Working with universities and other research institutions to build the cyber security regime pipeline through; competitive scholarships, fellowships, and internship programmes must be our preoccupation to attract top talent and develop systems that have command and control in our hands by which we must safeguard our national security' (2015 Cyber Symposium, David Mahlobo speech).

Ultimately, with knowledge being power, the research also aims to give a glimpse into the world of cyber security and techplomacy, and how this factor both safeguards national security and ensures the greater participation of the African agenda within the cyber domain, both on the African continent and the world as a whole. Currently, the technology patent capitals of the world include New York, London, Berlin, Beijing and Tokyo. How many African cyber patents are registered within these locations is important. It is thus imperative that cyber security is pursued both as a means to foster the economic benefits of the cyber regime and also to safeguard the cyber network from possible breaches and unintended consequences. Ultimately, this research will propose techplomacy as an emerging angle of analysis. Major technological pioneers such as Bill Gates 'Microsoft' and Elon Musk's SpaceX technologies-these players as the producers of tech within the technological realm have become important players in the emerging age of cyber and artificial intelligence technologies, gone are the days of only global politicians being the main actors within the global arena. This research then seeks to offer a new techplomacy perspective whereby leaders of the tech sector

act as the producers of technology and governments as the regulators of technology- engage in relations and partnerships together under the banner of techplomacy. whereby partnerships between governments and the private sector drive increased cyber security, human capacity and critical infrastructure protection. Through this activity are states able to adapt and mitigate the risk of the cyber domain, thus securing their cyber realm.

Cyber security is thus a necessary factor to fuel development, but also the most potentially devasting evil if not implemented correctly as it may impede a state's ability to provide services to its citizenry.

According to the Wilson Centre, at present the median age in Sub-Saharan Africa is 19 years of age. Ultimately, highlighting that the African continent has an exceptionally young population. Young people also eagerly embrace technology, incorporating technology through the use of mobile devices, E-education platforms and business dealings. While this is a positive factor this can also be an exceptionally negative factor as well, encompassing hard-hitting consequences for states.

Hendrik Zwarts, Jaco Du Toit and Basie Von Solms highlight how Africa risks the emergence of 'cyber ghettos', which are defined as spaces where cyber harm may become prevalent and from where cyber-attacks can be easily launched (Zwarts, Du Toit and Solms 2022,34). Felix E. Eboibi also draws attention to how Africa has been nicknamed as a haven for cybercrime and cybercriminals (Eboibi 2020,80). Authors Iginio Gagliardone and Nanjira Sambuli draw upon the same question as they ask has Africa become a new safe harbour for cybercriminals? (Gagliardone and Sambuli 2015,3-4). Many African states have exceptionally high inequality and unemployment rates, with young people making up the bulk of those statistics. As variables such as a tech-savvy youth, unemployment and lacking national cyber security intelligence agencies and legislation find a means of co-existence; this may see young people resort to employing their technological skills as a means of either accessing an income or engaging in protests against the state using cyber means referred to as 'hacktivism'. Hence, what does this mean for the African continent is the fundamental question, do we risk becoming a haven for cybercriminals, similar to how a failed state lacking effective institutions becomes a haven for non-state actors such as terrorist or organised criminal groupings?

Cyber Legislation and Diplomacy of the Coming Age.

With the spark of cyber conventions and agreements such as the Malabo Convention which is the 'African Union Convention on Cyber Security and Personal Data Protection', which is aimed at protecting information systems and developing cyber common norms. The United Nations recently released draft legislation on cybercrime known as the ' United Nations Treaty on Countering the Use of Information and Communications Technologies for Criminal Purposes', which will be debated in the August session of the UN session in New York, according to Summer Walker; states will ultimately be debating the very first global cyber treaty, with a focus on criminality and state powers to address the crime (Walker 2023,1-2).

With policy makers, regional and international organisations, including civil society organisations scrambling to prepare and adapt to the coming cyber revolution. This sparks the question of whether we see the crafting of cyber diplomacy, in a similar fashion as the world now sees the emergence of climate diplomacy given the challenges of the climate crisis. The research ultimately seeks to fill this gap. Hendrik Zwarts, Jaco Du Toit and Basie Von Solms define cyber diplomacy as diplomacy within the cyber domain and the usage of diplomatic means, including the performance of diplomatic functions to secure national cyber interest concerning the cyber-space (Zwarts, Du Toit and Von Solms 2022,341). As mentioned before, disruption needs planning, and at present the world and Africa need capable, well-informed and experienced cyber-diplomats as a means of securing the continent's place and interest.

When discussing the cyber domain, Petrus Duvenage and Sebastian Von Solms, make mention that cyber security entails the concepts of cyber offensive and cyber defensive systems and protocols (Duvenage and Solms 2015,46). This is essentially where the cyber power of a state is measured or tested. Authors Julia Voo, Irfan Hemani, Simon Jones, Dan Cassidy and Anina Schwarzenbach refer how cyber power is considered the fifth domain of statecraft, after land, sea, air and space capability (Voo, Hemani, Jones, Cassidy and Schwarzenbach 2020,2-3).

African Narrative on Cyber Power and Development.

Joseph Nye, argues that how while there is no commonly agreed-upon definition of cyber power, cyber power within the cyber domain can be thought of as states using resources to prop up cyber capability as a means of launching cyber operations against a nation-state or non-state actor to gain strategic advantage over an adversary; or having cyber means to resist a cyber-attack on critical systems in the event a state finds itself under attack by an adversary state or a non-state actor (Nye Jr 2010,3-5).

Ultimately, with cyber power resisting notions such as cyber offence and cyber defence, this research aims to grapple with where exactly the cyber security complex of African states fits into, given the reality that many African states lack both cyber offensive and defensive capability. This leaves a notable gap in the literature. Perhaps a gap to then fill within the context of this research rests upon asking, what is the developmental cyber power of African states. Petrus Duvenage, Wilhelm Bernhardt and Sebastian Von Solms draw upon how the Global North's terming of cyber security power has predominantly remained one dimensional revolving around 'offensive cyber power', instead they propose the notion of a cyber power triad encompassing offensive, defensive as well as developmental dimensions of cyber power; this would be more broadly encompassing of African states strategic national objectives while ensuring that the limited resources devoted to cyber security are utilised optimally (Duvenage, Bernahardt and Solms 2022,78). It is also highlighted that developmental cyber power entails bringing together a state's collective cyber capacity that is potentially relevant to its national priorities, as this capacity has human, institutional, technical and infrastructural facets.

Petrus Duvenage, Wilhelm Bernhardt and Sebastian Von Solms also argue how cyber power relies upon necessary national strategy objectives and measures, including the allocation of national resources and effort; in retrospect optimising cyber power demands that resources be shared and as far as possible serving all three power dimensions (Duvenage, Bernhardt and Solms 2022,178-183).

Developmental cyber power is ultimately about pooling societal resources to secure cyberspace and ensure an effective and adaptable national cyber security strategy.

Developmental cyber security also highlights the argument that yes, while certain African states may not have the necessary cyber capability now, with investments today how could these outcomes increase cyber power in the near to far future on the African continent? Gracie Sebina and Amy Mutua draw upon how 70% of cyber technology utilised in the South African Development Community region is provided by South Africa (Sebina and Mutua 2023,13-15). Ultimately, a worthy field of exploration could be, what would cyber power look like if SADC states collectively pool resources and sovereignty to better fortify the African continent's collective cyberspace.

Iginio Gagliardone and Nanjira Sambuli add that in striving for cyber resilience states should pursue three strategies based on emulation, extraversion and enculturation; with emulation entailing the adoption of internationally recognised standards to withstand cyber-attacks, extraversion revolving around a state turning unequal relations within the cyber domain to further its cyber agenda, lastly enculturation is built upon using/developing local systems as a means of safeguarding critical infrastructure systems (Gagliardone and Sambuli 2015,1-2). While African states are welcome to pursue any of the mentioned three strategies it is best to have a blend of the three as a means of achieving a comprehensive cyber security framework.

Iginio Gagliardone and Nanjira Sambuli even argue how emulation, extraversion and enculturation are not mutually exclusive, but on the contrary function best when these strategies co-exist alongside one another. A worrying reality according to Bhaso Ndzendze, Faten Aggad and Olumide Abimbola is the fact that on the entire African continent, Egypt is the only state which has developed a national cyber security strategy aimed at dealing with the possible threats posed by artificial intelligence (Ndzendze, Aggad and Abimbola 2021,5-7).

Influence of Outside Powers to the African Cyber Domain.

This literature review would be incomplete without mentioning the impact of outside powers on the African cyber domain. Just as the influence of outside powers in the Middle East and North Africa has often resulted in bloody wars, so too does the role of outside powers risk Africa falling victim either directly or indirectly to acts of cyber warfare. For starters since the trade war between the United States and China, Africa has found itself in the middle of an extremely futuristic war; with a

technological battle occurring between technology producers in the U.S. and China. This leaves Africa vulnerable as the continent relies upon both the American and Chinese tech market as a source of cyber development infrastructure. Matthew La Lime, Nate Allen and Tomslin Same-Nlar draw upon how technology creates spreading vulnerabilities that arise from the technical nature of cyberspace (La Lime, Allen and Nlar 2022, 15).

Ndeapo Wolf, Deon Cloete and Jan Hofmeyer highlight how as global powers find themselves in a race for technological dominance, this will have profound implications for the choices that policymakers in Southern Africa make (Wolf, Cloete and Hofmeyer 2022,5). Three dominant tech models exist on the African continent, these include the American, European Union and Chinese State models.

Ndeapo Wolf, Deon Cloete and Jan Hofmeyer mention how the American model is largely based on surveillance capitalism, where big tech players hold tremendous state-backed power, the Chinese model is a centralised state model in which state-owned companies with strong links to the Chinese Communist Party compete for cyber influence on the African continent; while the European model aims to position itself strategically as an actor in shaping normative contours that aim to guide digital and innovation development and research (Wolf, Cloete and Hofmeyer 2022, 5-10). Ultimately, African cyber security policies also face an uphill task of having to navigate between these macro-environmental factors.

When closely examining the Kenyan and Ethiopian case studies within the research, what will be highlighted is the influence of outside powers on the internal cyber domain of the Ethiopian and Kenyan cyber landscape. It will be highlighted how rival states have now begun incorporating cyber tools as a means of achieving foreign policy objectives and fuelling instability against targeted states, which in the context of this research are Ethiopia and Kenya.

The spreading of misinformation and disinformation can also be classified as a cyber incident, as this activity relies upon cyber technology as a means of distorting information and spreading propaganda. United Nations policy brief on a ‘New Agenda For Peace’ highlights how technology and warfare have been linked intrinsically throughout human history, while the expansion of powerful software tools that can proliferate and distort content almost immediately and massively

heralds a qualitatively different, new reality; non-state and nation-states have misused technology to coordinate and plan cyber incidents, including cyber-attacks with the objective expanding recruitment while inciting hatred and violence (UN 2023,5-6).

Various forms of misinformation and disinformation pose a threat to many states on the African continent. As propaganda is largely aimed at changing the hearts and minds of civilians, while also seeking to control the minds and hearts of civilians. With almost three-quarters of the African continent embarking on elections between 2023 and 2024, during periods of coups and elections, cyber incidents such as misinformation and disinformation increase. An interesting factor within the African cyber domain entails that African states that have varying cyber security policies, systems and legislations in place it is aimed at protecting and safeguarding critical systems and data information; essentially it is aimed at protecting something. While African states largely lack cyber systems, legislation and cyber security policies often have nothing to protect against due to not having advanced or adopting increased cyber systems; while these states are safe from conventional cyber incidents such as cyber espionage and cyber-sabotage find themselves exceptionally vulnerable to acts of misinformation and disinformation, including cybercrimes. This is a crucial distinction, as a recent report by Liquid Cloud and Cybersecurity highlights how cyber security development is not occurring at an evenly distributed rate on the African continent, in essence, development is occurring in specific pockets on the African continent (Liquid Cloud 2022,20-28). This essentially means that cyber resilience cannot be measured evenly, as certain corners of the African continent are more resilient than others based on their rate of cyber development. This also means that the threat landscape on the African continent is vastly diverse, as states with cyber systems are more likely to become victims of cyber sabotage or cyber espionage given that they have data and critical systems to protect; which provides incentive for nation-state and non-state actors to gain access, while states with no cyber systems and nothing to protect often find themselves victims of cybercrimes and acts of misinformation and disinformation.

It is then clear within the literature review- what threats Africa has to grapple with, that the cost of entry into the cyber domain is low, bringing with it both challenges

and opportunities. States should then leverage what they can and protect against what is viewed to be a threat.

Theory:

For this research project, two theoretical schools will be utilised, which include, securitisation theory and techplomacy.

Securitisation Theory:

Iktisedi Isletmesi, defines securitisation theory as the determination of a threat, or the construction of a threat, in which a securing actor constitutes a factor as a security issue that needs to be securitised as a means of safeguarding national integrity and security (Isletmesi 2020,15). The decision is often taken by high-level political or security actors. Ultimately the cyber domain should be constituted as a security issue, which must fall into a special category of existential threats.

Rita Taureck draws upon how successful securitisation consists of three steps, which include identification of existential threats, emerging action and effects on inter-unit relations by breaking free rules; securitisation according to Taureck is also based on power and capability and ultimately the means to socially and politically construct a threat (Taureck 2006,3-6).

For adequate securitisation to occur political or intelligence elite must convince the populace that an issue is a security threat. Iktisedi Isletmesi argues how political elites must convince the audience that an issue is an existential threat to security as a means of legitimising the extraordinary measures taken to overcome or safeguard the threat (Isletmesi 2020,2-3).

Ultimately the collection of speeches by policymakers where an issue is brought into the public domain is the first step in gaining traction for a security issue as a means of securitizing the threat.

During a Question-and-Answer session of parliament in 2017, Democratic Alliance MP Dirk Stubbe had asked then Minister of State Security David Mahlobo for comment on internet security in South Africa. Mr Mahlobo answered as follows: ‘We maintain that information sharing via the electronic web or cyberspace has revolutionised our world and how we interact with each other, however, on the same

breath, there are real threats that have manifested themselves in the same space, which if left unchecked can destabilise our use of this space and result in untold harms to individuals, corporates and governments' (Parliamentary Question and Answer sitting, 2017).

Former South African Minister of Communications Yunus Carrim, at the launch of the National Cyber Security Advisory Council (NCAS), spoke upon how 'with increasing number and sophistication of cyber security threats, including online scams, data theft and other threats, the role of NCAC has become more important than ever'(NCAC Launch 2013).

In the opening of the 17th Internet Governance Forum, Ethiopian Prime Minister Abiy Ahmed highlighted how ' rapidly evolving digital landscape allowing us to produce massive amounts of data, this requires cautious optimism especially around data governance and cyber security, countering imbalances in ownership of submarine cables, terrestrial fibre-optic cables, data centres are dependencies that risk jeopardising the state; hence, the focus must be on building trust, equity and security in the cyberspace' (17TH Internet Governance Forum,2022).

Securitisation of a threat revolves around key sectors which include, the military, political, economic, societal and environmental sectors. Barry Buzan points to how the military sector entails the ability to fight wars, the political sector is about relationships of authority, the economic sector is about trade production and finance, the societal sector is about the longevity of shared identities, while the environmental sector is about human activity and the biosphere (Buzan 2021,415-418).

Drawing upon securitisation theory one can see how it is closely linked to the cyber domain. For one, within national cyber security strategies, it is the military and intelligence services that must guard against and respond to cyber incidents such as cyberwarfare, cyber espionage and cyber-sabotage. Ultimately acts of cyber-offence and cyber defence are the prerogative of the military sector as a means of safeguarding critical cyber infrastructure. It is also a key factor that cyber is but another arm of military strength, alongside conventional military power bases revolving around the ability to engage in warfare on land, sea or air. Within the South African context, the cyber command centre responsible for monitoring and capacity

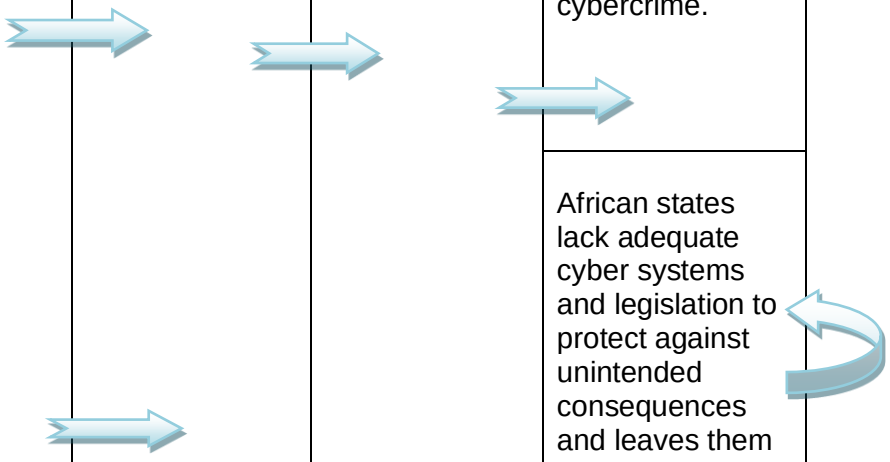
building of the national cyber security strategy is run on a command base protected by the South African National Defence Force (SANDF).

Touching on the political sector, cyber security is an exceptionally political phenomenon. States, by virtue of existing within the global system, are compelled to cooperate; more especially on issues which exist within the security domain. According to Iktisedi Isletmesi, within an International Relations context, relationships are guided by national interest (Isletmesi 2020,5-7). Key cyber security agreements such as the Malabo Agreement, UN Cyber Treaty and African Union Convention on Cyber Security and Personal Data Protection, all relied upon political negotiation and statecraft as a means of eventually becoming key cyber legislation.

In line with the economic dimension of securitisation theory, cyber security is also a key determinant of threat or success to this sector. As African states aim to adopt or leverage technological advances such as fin-tech, agri-tech and the connection of key state services to a technological grid, all these systems must be safeguarded by strong cyber systems, capable of protecting against cyber sabotage. In the event of a cybercrime targeting fin-tech groups, or a nation-state attacking critical energy grids, this could lead to economic distress or complete collapse. Therefore, strong and effective cyber systems are essential if the African continent is to employ emerging technologies as a means of leapfrogging development.

Process Tracing of cyber security

Trigger	**Causal Process**			**Outcome**
	Part 1	**Part 2**	**Part 3**	
Emergence of disruptive technologies and the rise of the data economy.	African states adopt cyber technology with the objective of leapfrogging development.	Technology brings with it unintended consequences, cybercrime, cyber espionage, cyber sabotage.	African states adopt cyber security systems and cyber legislation with objective of safeguarding against cyber espionage, cyber sabotage and cybercrime.	Securitisation of the cyber domain.
			African states lack adequate cyber systems and legislation to protect against unintended consequences and leaves them vulnerable to acts of cyber espionage, cyber sabotage and cybercrime.	



Process Trace: Compiled by student.

Techplomacy:

In 2017 Denmark became the first state to appoint a technoplat, given the rapid developments within the cyber space. A draft report by the Ministry of Foreign Affairs in Denmark, described the need for the development of techplomacy as a result of global technology corporations and other digital actors influencing almost every quarter of society, revolving around citizens, everyday life, including social as well as work life, which also encompasses Danish security to a vast extent that is capable of surpassing the influence of many countries including Denmark (Foreign Ministry 2020,1).

Major powers such as the United States, United Kingdom, and China have for decades been powers that have charted the trajectory of global affairs within the global political area. Hence, diplomacy as a means of undertaking statecraft has been the tool of trade when powers undertake relations amongst each other and other nation-states.

Ultimately with the emergence of the fourth industrial revolution, tech firms including leaders of technology firms have become important players within cyberspace, and figures such as Elon Musk and Mark Zuckerberg have become vastly influential persons, who now command authority. With cyberspace being a borderless entity, tech firms as producers of technology capable of undermining national cyber security and stability; and states which are also producers and legislators of cyber technology have to cooperate and find channels of working together to fight common cyber incidents such as malware, ransomware and other technological anomalies. This is why just as states employ diplomacy to engage each other and co-exist within the global area, states and tech firms must employ techplomacy as a means of safeguarding cyberspace and developing cyber tech for positive usage.

The Danish Ministry of Foreign Affairs defines diplomacy as a craft and exercise of influence between sovereign nation-states which includes multilateral organisations, however, the 4th industrial revolution challenges these traditional concepts of power, on a national, regional, and global scale (Danish Ministry of Foreign Affairs 2020,1).

Shaun Riodan and Mario Torres Jarrin highlight how diplomacy engages with technology along three vectors: agency, process, and content, with internet and tech corporations labeled as geo-political actors operating within cyberspace (Riodan and Jarrin 2020,3). Agency involves the ability of both tech firms and states to co-exist and exercise influence as a means of undertaking processes of protecting cyberspace, which also involves content exploring what technology poses an existential threat to both tech firms and states. The technological revolution largely entails that states now share power and influence with tech firms as a means of fostering greater cyber resilience.

Cyber security can be undermined by information warfare and conflict within cyberspace, which in turn poses great risk to the national security of a state. This was seen in several African states, but more broadly in states all over the world. Russian bots have often been responsible for cyber espionage and cyber sabotage during election periods aiming to swing public opinion either to or away from certain presidential candidates. This was done on a grand scale during the 2016 American election when Russian hackers influenced voters via search engines and Facebook platforms intending to swing the electorate in favour of Donald Trump. Kathleen Hall Jamieson draws upon how undecided voters were particularly influenced by Russian hackers (Jamieson 2019,120-122).

Hence, tech firms as geo-political actors must work hand in hand with states via techplomacy as a means of securing cyberspace. Cyber governance according to Shaun Riordan and Mario Torres Jarrin should be a multistakeholder approach, where techplomacy guides relations between key stakeholders, while cyber governance must be implemented via mechanisms that involve non-state and state actors and include other organs of society such as non-governmental organisations and cyber technicians (Riordan and Jarrin 2020,6).

Jeppe Kofod former Foreign Minister of Denmark uttered the following remarks: ‘We’ve been naïve for too long about the tech revolution. We need to make sure that democratic governments set boundaries for the tech industry and not the other way around (Tech Ambassador of Denmark 2017,1-3).

Brad Smith, President of Microsoft Corporation mentioned that ‘what we need is a Digital Geneva Convention. We need a convention that will call on the world’s

governments to pledge that they will not engage in cyber-attacks on the private sector, that they will not target civilian infrastructure, whether it's of electrical or economic or even the political variety' (RSA Security Conference 2017).

Techplomacy came to life when tech firms frustrated with the pace at which global institutions and states were taking to regulate harmful technology in cyberspace, came together and agreed on a Microsoft-initiated cyber security convention, according to the Lee Kuan Yew School of Public Policy this brought together 80 tech firms, including Facebook, Dell, and TrendMicro; with the convention aimed at promoting security, stability, and resilience in the cyberspace (Kuan Yew School of Public Policy 2017,1).

As a result of the emergence of a tech industry coupled with their vast control over big data, and cyber systems, digital connectivity essentially sees tech firms controlling the capabilities integral to a functioning society. Hence, by crafting a complex and extremely connected information and infrastructure landscape, national cyber security threats have evolved with big data being weaponised for war.

Techplomacy has become ever more crucial as a means of formulating industry-driven gold standard technological policies.

South Africa currently possesses an extremely developed private sector with vast expertise in cyber security. Hence, the country has taken meaningful steps to incorporate and even cooperate with the private sector as a means of safeguarding the cyber domain. More initiatives like these are needed on the African continent. A technical report produced by the International Monetary Fund (IMF), draws upon how the South African financial system and banks have a long history of incorporating technology into the business practice as a strategic practice (IMF 2022,5-10). Ultimately, establishing cyber strategies, frameworks, and governance are routine practices in driving cyber resilience within the private sector.

The Lee Kuan School of Public Policy argues that states lay down the following factors influencing the state of techplomacy: Tensions and rivalry between tech firms and states, with many governments wanting to put caps on the power of tech firms; rising techno-nationalism in cyberspace, with states attempting to exert and preserve

their sovereignty through the cyber domain (Lee Kuan School of Public Policy 2017,3).

Ultimately, African leaders should be utilising cyberspace to train and develop a body of technoplats as a means of negotiating the African agenda on cyberspace.

The Interaction of Securitisation and Techplomacy:

It is relatively easy to elaborate upon how techplomacy and securitisation need to co-exist as states seek to secure their critical infrastructure via developing and adopting cyber security systems. Transnational issues such as climate change and the rise of artificial intelligence-phenomena such as these will not be solved within the borders of a single nation-state, regardless of the economic and military power the state may possess. This is pivotal given that innovation to addressing these challenges largely occurs within the private sector, hence, as both governments and private sector corporations encounter risks to their national security and profitability margins, the need to form healthy lines of cooperation and information sharing between the state and private sector is critical in safeguarding the cyber domain of a state.

National security entails the security of a state, its citizens, the economy as well as institutions and is largely regarded as the duty of an effective government. States have the responsibility to cooperate on issues that pose a threat to society, while private sector corporations have a responsibility toward their shareholders to ensure profitability and a flourishing business. Ultimately cyber incidents such as ransomware and malware pose risks to both private sector corporations where technological development occurs and states as the regulators of the cyber domain. Cyber incidents also pose a great risk to economies, citizens, and institutions, hence, in this reasoning is where the justification comes into play that states and private sector tech corporations must strengthen cooperation between each other as a means of fostering the securitisation of the cyber domain. Factors such as political, economic, and military power including diplomacy especially techplomacy are the best means through which states can safeguard their critical cyber infrastructure.

If a state is hit with a massive cyber incident such as in Estonia in 2007 where a Russian cyber incident shut down the state's entire electricity grid this ultimately entails that conditions for private sector innovation and profitability are put at risk as

well. Energy is needed to drive innovation, while a consumer base is needed to drive profitability. Hence, in the case where a state is hit with such a cyber incident, profitability and access to energy are constrained. Securitisation of the cyber domain is not just the responsibility of the state but cannot occur without the input of the private sector as well.

African states in particular may pursue emulation strategies to that of states in the Global North when it comes to fostering greater cyber security levels. The formation and adoption of National Pride Industries can be critical to securitising the cyber domain and fostering a relationship between the private sector and the government. States may partner with tech startups and support innovation and production of cyber technologies via tax breaks and concessions, including fostering private-public partnerships in human capital development. The 2021 Global Startup Ecosystem Report labeled Cape Town as Africa's Tech Capital; Cape Town has even been nicknamed 'Silicon Cape'-where 60% of African tech startups are based. This presents a unique opportunity for South Africa to undertake both techplomacy and securitisation. South Africa could give this sector National Pride status and work alongside these businesses to foster greater human capital and cyber skills enhancement, while also investing in tech innovation that could see South Africa develop local homegrown cyber systems and human capital. This will ultimately create synergy between the private sector and government (techplomacy), while also developing systems to secure the South African critical system infrastructure domain (securitisation).

It is also important to note that the cyber domain is no longer an exclusive epistemic domain comprising of military intelligence personnel and computer scientists, but a domain compromising of a diversity of actors-which include hackers, state agencies, tech corporations, and many other illicit criminal networks. Hence, techplomacy addresses this gap in the sense that it stands to bring the two main actors operating in the environment together which are the state and tech corporations. Authors Fabio Cristiano, Xymena Kurowska, and Dennis Broeders argue that cyber security requires expertise about how to deter, patch and govern or prosecute exploits of the technical vulnerabilities as issues of both national security and global governance (Cristiano, Kurowska, and Broeders 2024,4).

The need to safeguard the cyber domain can also be traced back to the writings of the great Niccolo Machiavelli. Per Jansson argues that Machiavelli believed that there are two manners in which actors could go about fighting, which is either by law or by force; the former according to Machiavelli is normal to men, while the latter is to beasts (Jansson 2018,347). Hence, Machiavelli says that a prince must be both physically powerful and imposing but also simple-minded and defenceless against traps, hence, the notion of the lion and the fox is employed by Machiavelli to show the characteristics that should be embodied by a prince; as strong and fierce as a lion but as sly as a fox, combining the two to outsmart the enemy (Hans Baron1961,99-105).

Ultimately, a state should develop a strong cyber security framework of systems using both the qualities of the fox and the lion. Within the cyber defence domain, a state's cyber security system must be like the fox; entrusted with the duty of being cunning while being able to anticipate an attack or dodge an attack in the event of a cyber intrusion. In the cyber offence domain where a state must launch a counter cyber-attack in the event of being targeted by adversary states or non-state cyber actors, this is when a state's national cyber security framework must embody the traits of the lion; the cyber strength of a state must then be capable of launching an attack against cyber intruders that must employ cyber power as a means of derailing any plans at present or future cyber-attacks undermining a state's cyber security networks. Machiavelli argues that law and force should be mechanisms in which a prince maintains power (Hans Baron 1961,99), ultimately cyber legislation including a techplomacy framework and strong technical national cyber security capacity must also combine both force and law as a means of safeguarding a state's cyber domain.

Part III: Case Studies

Case Study 1: South Africa

State of Cyber Security in South Africa:

At present South Africa, employs legislation, task teams and cyber policy as a means of safeguarding its critical cyber infrastructure. According to the State Security Agency Government Gazette dated December 4th 2015, National Critical Information

Infrastructure entails all components which involve ICT systems and networks that are essential to the adequate functioning of the Republic; the State Security Agency thus also acknowledges that South Africa is still too much of a consumer of ICT's and is vastly dependent on technology manufactured overseas to safeguard its cyberspace, therefore there is a need to fast track the production of Indigenous technologies (State Security Gazette 2015,6-13).

Local Cyber Legislation:

South Africa has implemented a range of legislation to mitigate and adapt to the challenges and opportunities of cyberspace. The Cyber Security Policy of South Africa 2009, which has mandated the adaptation of a cyber inspectorate as a means of fostering the creation of safe, secure cyberspace for the consumer, business and government, this was done in line with Resolution 57/239 of 2002 of the United Nations Cyber Resolution Act, which identifies the creation of a global culture of cyber security; awareness, responsibility response, ethics, democracy, risk assessment, security design and implementation of cyber securing management strategy (Cybersecurity Policy of 2009, 8-13).

The Electronic Communications and Transactions Act of 2002 was adopted to curb cybercrimes, the Act entails that the Minister of Communications must implement projects aimed at developing human resources needed for the safeguarding of cyberspace (Electronic Communications Act 2002,12).

Cyber Crimes Act of 2020 was implemented to curb cybercrimes undermining the national security of the South African state. This Act created mechanisms for addressing cybercrimes, such as the criminalisation of disclosure of data which can be harmful, while also mandating security agencies such as the SAPS and Hawks as bodies entrusted to investigating and gathering evidence to bring cybercriminals to book; the Act also outlines guidelines for working with foreign agencies with the aim of bolstering detection, prevention and mitigation of cybercrimes.

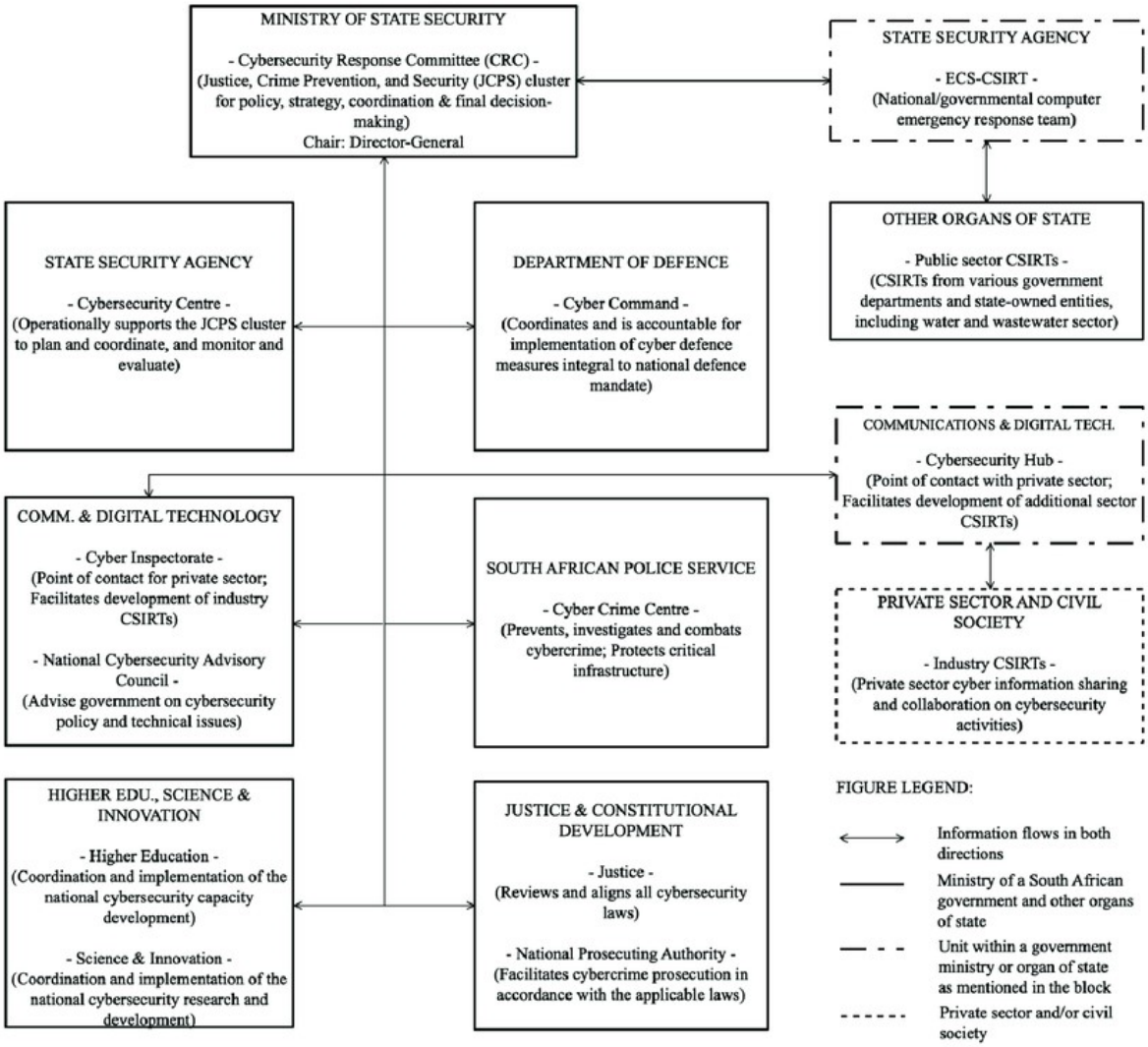
South Africa also remains a signatory of regional and international conventions aimed at securing cyberspace, which include the International Cooperation Convention on Cybercrime (Budapest Convention), Model Laws on Cyber security Agreement Southern African Development Community, MoU on Cyberspace under India, Brazil

and South Africa Grouping (IBSA), and Cyber Cooperation Agreement and Partnership involving South Africa, Iran and Russia.

In 2012 South Africa adopted the National Cyber Security Policy Framework (NCPF), Ewan Sutherland highlights how the NCPF entailed the creation of 'South Africa's National Computer Incident Response Team (CSIRT), which collaborates with stakeholders from the private sector, civil society and the public to identify and counter cyber security threats (Sutherland 2017,84-87). This is a good example of where techplomacy currently functions well on the African continent. The NCPF also forged the creation of a JCPS Response Committee chaired by the Director General of the State Security Agency, where decision-making and strategy are formulated in the event of a cyber incident, the Department of Defence is also present within this structure with the main goal entailing combatting and protecting national security threats in form of cyber warfare, cyber-crime and other cyber incidents (Sutherland 2017,92). The cyber security centre where all these activities take place is located at the State Security Agency.

Another core function of the Cyber Centre according to the State Security Agency Gazette of 2015, is the core safeguarding of national cyber strategy, where the cyber centre must also facilitate analyses of cyber security incident trends globally, and identify vulnerabilities within the cyber systems of the state, while also engaging in information sharing as a means of protecting national security and threat response coordination, regular testing and assessment of National Critical Infrastructure it also forms part of the Cyber Centre chaired by the JCPS (State Security Agency Gazette 2015, 5-9).

The state of cyber legislation and protocol guidelines in South Africa seem to be exceptionally outdated. This poses an extreme security risk, as the cyber landscape of threats is constantly changing and sophisticated. Cyber frameworks and protocols from almost a decade ago would prove to be vastly incapable of responding to these threats. According to a report by journalist William Brederode, South Africa only has 64 civil servants focused and trained within the field of cyber security (Brederode 2024,3-5). This precisely highlights the vast shortage of technical capacity within the South African cyber security framework.



South African National Cyber Security Governance Structure

Source: Cybersecurity Policy and the Legislative Context of the Water and Wastewater Sector in South Africa 2020.

Cyber Incident: Transnet 2021

In July 2021 Transnet declared that the entity had been hit by a mass cyber incident. Brigid Gesami and Gregory Kasembeli highlight how a ransomware attack encrypted every Transnet file and system which resulted in the entity being unable to process cargo electronically (Gesami and Kasembel 2022,2-3). This was a major cyber-attack, which crippled major Transnet ports of Cape Town and Gqebeha, with the Durban port being the hardest hit.

This was a ransomware attack also known as cyber hostage-taking, where attackers encrypted files as a means of extorting a ransom from the entity in exchange for the release of the files. Brigid Gesami and Gregory Kasembeli argue that how 60% of South Africa's imports are shipped in from the Durban port, cargo flow essentially came to a halt (Gesami and Kasembeli 2022,3-5). The Global Agricultural Information Network Report also highlight how 65% of Southern Africa's containerised trade flows through the Durban harbour, as a result of the cyber-attack processing times for cargo increased as it had to be done manually at a rate of three containers per hour; which ultimately, caused a backlog due to the large build-up of cargo, Transnet was hit with the attack on the 22nd of July and only restored systems on the 29th of July 2021 (Global Agricultural Information Network Report 2022,6-11). Map one is a visual depiction of the Transnet trade lines utilised as a means of transporting goods and materials from South African ports to the rest of Africa, all these trade lines located within the SADC region experienced disruption in value chains as a result of the cyber incident.

Map 1: Transnet Trade Lines



Source: LTPF Chapter 7: Africa Transport Infrastructure Planning Transnet 2016.

This can be viewed as an attack that targeted critical infrastructure, as a result of its economic consequence. This disruption also undermines President Cyril Ramaphosa's commitment in May 2021 to implement an R100 Billion infrastructure development project aimed at making Durban the best functioning port on the African continent.

For eight whole days, port trade came to a standstill, with goods not being able to access the South African market or the broader Southern African market. Tefesehet Hailu Sime highlights how the proliferation of digitisation, automation and operational integration in the maritime sector has resulted in the industry becoming exceptionally vulnerable to cyber-incidents (Sime 2023,8).

As procedure law enforcement and relevant agencies were notified of the attack, yet what was starkly interesting is that Transnet technicians undertook the activity of responding to the ransomware attack. Under the NCFP framework, this attack should have been placed within the de-restriction of the Cyber Command Centre, where relevant agencies should have been making efforts aimed at countering the attack. This represented a break in procedure, a factor that could have caused this break in procedure is the fact that during this period, South Africa but provinces of Kwazulu-Natal and Gauteng in particular were griped by violent acts of violence, looting and protest, including attacks on physical critical infrastructure; which saw the deployment of the SANDF to quell the violence as a result of the SAPS and Metro Police agencies finding themselves unable to disrupt the flow of protest. Hence, law enforcement and intelligence agencies could have essentially been spread too thin, to deal with the complexities of the ransomware attack on Transnet. Cyber hackers may have recognised this vulnerability and viewed it as the perfect time to strike as the country was already in a state of instability.

As a result of Transnet being hit with this cyber incident, causing a slowdown in the processing of cargo, trade essentially took a knock as well, as this event caused an interruption to regional value chains, thus causing a macroeconomic shock. A macroeconomic shock according to IMF economists Patcharaporn Leepipatpiboon, Chiara Castrovillari and Tomohide Mineyama can be defined as a sudden and unanticipated event that causes a sudden and significant impact on the economy (Leepipapiboon, Castrovillari and Mineyama 2023,48-51).

Transnet's 2021 Integrated Report highlights how the SOE, links trade between Botswana, Lesotho, Mozambique, Namibia, Swaziland and Zimbabwe, via its Transnet Transportation Model (TTM) which is a model that produces flows of trade on the rail network, cross-border and through the port system; through this process Durban handles over 86-Million tons of cargo per annum and is the leading port in the

Southern African Development Community Region (Transnet Integrated Report 2021,419-422).

The ransomware attack ultimately resulted in a trade downturn as raw materials and supply value chains could not enter or exit the region, this alone cost the South African economy nine billion rands and slowed trade in the entire SADC region. Brett Van Niekerk draws upon how this cyber-incident occurred during a key exporting period for the exporting of citrus fruit, thus causing delays in citrus reaching their intended markets (Van Niekerk 2023,171). According to the Centre for Strategic and International Studies, Transnet reportedly declared the attack 'force majeure' (CSIS 2022,22). Force majeure is essentially a legal term which implies that an entity does not accept liability for an event of unforeseeable and catastrophic consequences.

Process Trace of Macroeconomic Shock as Result of Ransomware Attack:

Trigger	Casual Process			Outcome
	Part 1	**Part 2**	**Part 3**	
Transnet Hit with system disabling ransomware attack.	Transnet unable to digitally process cargo as a result of file and system encryption.	Build-up of cargo as a result of slow processing times, only three shipments per hour processed manually.	Disruption of value chains.	Macroeconomic shock
			Raw material cannot enter or exit South Africa and broader SADC region.	

Process Trace: Compiled by student.

As a result of Transnet declaring 'force majeure' in the wake of the cyber incident, this in reality highlights how Transnet and the South African cyber command itself had no intelligence as a means of pre-empting the cyber-attack. Hence, there was no cyber defensive capability shown in the wake of this cyber incident. Ultimately, Transnet demonstrated little cyber resilience as it took the entity nine days to fully restore system function. While there were no cunning evasive characteristics of the prince, there was at minimum some strength of the lion demonstrated as Transnet managed to gain entry back into its systems after eight days and did not have to pay a ransom. This ransomware incident did not only affect the South African market but also the broader African market as well. Tefesehet Hailu Sime draws upon how maritime transport in Africa is dominated by three key ports, which include: Tangier

port-Morocco, Port Said-Egypt and Durban Port-South Africa; hence, landlocked states are exceptionally dependent on these ports and will greatly be affected as well in event of a cyber-incident (Sime 2023,9-11). So, in essence, the ransomware incident that hit Transnet entailed not only ramifications for the South African economy but the broader African continent as well.

The attack on Transnet also resulted in a deviation from policy and procedure, an entire playbook exists under the framework of the South African Cyber Policy and National Cyber Security Policy Framework (NCFP), of what to do in the event of a cyber incident. The cyber command should have been leading efforts aimed at countering or mitigating the cyber incident, not Transnet system technicians. This ultimately, represents a failure of policy and action on behalf of all stakeholders involved, which cost not only the South African economy but the SADC regional economy as a whole. Grace Tabea Letseka draws upon how it is Transnet's ultimate responsibility to provide reliable port, rail and pipeline services as a means of promoting economic growth while guaranteeing supply security; the cyber incident locked the SOE out of its systems, fuelling disruption in the movement of cargo; which affected service delivery to citizens and harmed the economy (Letseka 2022, 36). Transnet thus demonstrated limited cyber resilience as it negated its responsibility of safeguarding supply chains and being a reliable driver of economic growth.

South Africa in the aftermath of the cyber incident showed a limited desire to bolster cyber-measures. The latest worrying reality is that the Department of Justice and Constitutional Development, which is also a member of South African Cyber Command was fined a total of R5 million by the Information Regulatory on the 2nd of July 2023 as a result of failing to comply with an Enforcement Notice: issued by the regulator on the 9 May 2023 (Information Regulator 2023,2). The Department of Justice and Constitutional Development was hacked twice between 2020 and 2022, resulting in 11 transactions being made on the department's behalf wherein a total of R10 million was stolen from the department by cybercriminals.

Ewan Sutherland also argues how South Africa while a signatory of the Budapest Convention is yet to ratify this convention on cybercrime, while South Africa also signed the African Union Convention on Cyber Security and Personal Data Protection 'Malabo Agreement' but is still to ratify it (Sutherland 2017,92). Ultimately, South

Africa does not seem to lack the legislation and capability to thwart a cyber incident but instead, there seems to be a lack of synergy between the development and implementation of cyber legislation and coordination. The state does although appears to lack the capacity to lead the prevention of cyber incidents/attacks by implementing standards and addressing the dynamic cyber security skills deficit. Cyber security has largely fallen within the parameters of security agencies, but securing public infrastructure is the responsibility of the entire state.

An adequate cyber security strategy would entail more than just a paperwork strategy, public investment is essential to bolster the state's ability to identify and attribute blame when incidents and attacks occur, irrespective of who is targeted, whether it be private or public sector institutions. A worrying reality is that the Critical Infrastructure Act of 2019, which is geared toward securing critical infrastructure against threats, makes no mention of cyber security whatsoever; this is disastrous given that all water, electricity and state systems are connected to technological systems, which if compromised via a cyber-attack would disrupt water, power and online systems for hours, days and even months. The Critical Infrastructure Act of 2019 lacks even minimal monitoring or evaluation of cyber security risks. This is exceptionally chilling given the dangers cyber incidents pose to South Africa's sluggish economy.

South African policymakers and intelligence agencies must ultimately realise that constantly being reactive and not proactive to cyber incidents is vastly unsustainable and puts the service delivery and economic livelihood of the country at risk in the event of catastrophic cyber incidents. Implementation and coordination of policy and activities of cyber offence and cyber defence must be beefed up. South Africa should also be asking what lessons we can learn from the Transnet cyber incident as a means of preparing the cyber system for future acts of ransomware and malware, and how to safeguard all critical infrastructures against such attacks. Crisis events always serve to bring down barriers undermining cooperation, hence, as the saying goes 'never waste a good crisis' but learn from it going forward.

Case Study Two: Ethiopia

'If the river's level drops, let all the Pharaoh's soldiers hurry and return only after the liberation of the Nile restricting its flow. To prepare the Ethiopian people for the wrath of the Pharaoh's'.

The cyber incident on Ethiopian critical systems is a rather unique case and one of the very few African cyber incidents where it was a state-backed act of cyber-warfare and where the cyber incident was in retaliation to a political and economic decision taken by the Ethiopian state. Konstantin A. Pantserev highlights how between June 17th and 20th the Ethiopian state was hit by a mass cyber-attack of cyber-sabotage. According to Ethiopian authorities, the attack was aimed at creating significant economic, psychological and political pressure on Ethiopia over the filing of the Nile River's Grand Ethiopian Renaissance Dam (Pantserev 2022,288-290). Uche M. Mbanaso argues how cyberspace is but a new arena where cyber-attacks can now complement state conflicts (Mbanaso 2016,1), while Suraj Chandrakant draws upon how there is also an emerging flirtation with cyber tools as instruments of foreign policy (Chandrakant 2022,174). This can be largely seen playing out within the context of the Ethiopia-Egypt geo-political tensions.

It would be useful then to provide some background information as to what were the leading factors that sparked Egypt's cyber warfare campaign against Ethiopia.

The geo-political tensions between Egypt and Ethiopia stretch back to the 1930's largely surrounding Ethiopia's age-old desire to construct a hydro-electric dam on the banks of the Nile River. Ultimately, Egypt is the Nile, and the Nile is Egypt, Ethiopia's planned construction of the Grand Renaissance Dam, is capable of drastically decreasing the water supply to the Nile River, which is the lifeblood of the Egyptian economy and national survival. Egypt relies on the river for agriculture and water consumption. About 90% of Egypt's water comes from the Nile, therefore a lack of water availability as a result of Ethiopian construction of the GERD is an existential threat to Egypt. According to authors M.A Ashour, Y.M. Rafaat and M.N Mohamed highlight how the Nile is Egypt's main water source, which is limited to 55.5 billion m3/year (Ashour, Rafaat and Mohamed 2009,270).

Ethiopia has sought to justify its building of the GERD by highlighting how it can produce large quantities of kinetic energy, capable of bolstering Ethiopian energy supplies and exports to other African states, thus acting as a source of energy and economic security for the Ethiopian state. This will, however, come at a cost to the Egyptian economy, which Ahmed Kamara, Mohamed Ahmed and Arturo Benavides highlight to be a loss of Egypt's available agricultural land and will cause significant disruption to the supply of food and other agricultural products, thus negatively affecting the Egyptian economy (Kamara, Ahmed and Benavides 2022,7-9).

In 1978 then President of Egypt made the stark remark 'We are not going to die of thirst in Egypt, we'll go to Ethiopia and die there instead'. Goitom Gebreluel also draws upon how the construction of the GERD is also a break in Egypt's millennia-long monopoly over the Nile waters (Gebreluel 2014,33-35).

The 1929 Anglo-Egyptian Treaty granted the United Kingdom control over the Suez Canal in exchange for Egypt and Sudan being given full authority and the right to Veto any construction upon the Nile River, hence, the United Kingdom effectively recognised Egypt's right to all water along the Nile, Ethiopia on the other hand does not recognise this treaty. Ayele Guro adds to this debate as he highlights how Egypt and Ethiopia sought mediation from several parties and institutions including the United Nations Security Council, African Union, European Union including the United States itself- which cut off monetary aid to Ethiopia when construction of the GERD commenced (Guro 2022,150-155).

With the outbreak of Arab Spring protests that eventually gripped Egypt and toppled then-Egyptian President Hosni Mubarak, Ethiopia commenced with the construction of the GERD as Egypt was in no position to counter the construction of the dam. Ethiopia sought to benefit millions in increased revenue as a result of increased electricity exports. The Monsoon season in 2020 saw the first filling of the GERD, coupled with the second filling in July 2021 and the third in July 2022, and as of September 10th, 2023, Ethiopia announced the completion of the filling of the GERD. Ultimately, one could define the existence of the GERD as an existential threat to Egypt and an existential necessity to Ethiopia.

This has drastically strained relations between Egypt and Ethiopia. Hence, on the 17th of June 2020, the Ethiopian Information Network Security Agency announced that

33,000 computer systems had been victim of an act of cyber-sabotage. While Ayele Guro draws upon how two groups of cyber hackers in Egypt coordinated the cyber-attacks, these two cyber groups are known as ‘ Cyber Horus Group’ and ‘Anubis’; these same groups publicly claimed responsibility for the attack, Tomslin Samme-Nlar draws upon how Ethiopian authorities traced the attack back to Egypt (Nlar 2020,1-2); in total thirteen government websites were targeted including several state institutions which include both public and private sector organisations (Guro 2022,46-49). Institutions affected included the Metals Industry Development Institute, Dawuro Zone, Ethiopian National News Paper, Ministry of Information and Technology, National Lottery Commission, Police Commission, Statistics Centre and Education Office.

Suraj Chandrakant Mohite highlights how the following messages were plastered on each of the 33 000 computer screens: ‘ They warned, engaging with Egypt in a war may cost you more than the lives of an Ethiopian people’, along with hashtags #God_Bless_Egypt, #God_Bless_Egyptian_President, including the statement of ‘if the rivers level drops, let all the Pharaoh’s soldiers hurry and return only after the liberation of the Nile restricting its flow. To prepare the Ethiopian people for the wrath of the Pharaohs’ were slogans were displayed on each affected computer system (Chandrakant 2022,174).



Source: easternherald/2020/Egypt-Cyber-Attack-Ethiopia

This is also an example of how within the cyber domain the principle of collateral damage can also occur, as a result of strained relations between Egypt and Ethiopia and the emergence of this cyber-attack, the attack did not only affect the Ethiopian state but also the economic and educational institutions as well. This ultimately, draws upon how cyber-attacks can include deeply catastrophic economic and psychological effects as well. The Ethiopian cyber-attack can then be classified as a malware attack, as systems were deliberately sabotaged with no intent of demanding a ransom in exchange for the de-encryption of system files and operations.

This form of coercive diplomacy is ultimately a largely unique but still unconventional form of achieving foreign policy objectives, especially on the African continent. This should also act as a warning to states that in the future geo-political disagreements could potentially attract acts of cyber warfare. One could also assert that this could be seen as 'hawkish behaviour'. Andrew Scobell draws upon how a state may employ hawkish methods, which entail aggressive behaviour short of war to influence an opponent's change in policy (Scobell 2003,11-12). Ultimately, Egypt's hawkish warlike statements directed toward Ethiopia and its cyber-warfare campaign against Ethiopia can be seen as instruments short of a direct warfare campaign but still aggressive in its aims of influencing a change in Ethiopian policy concerning the GERD.

Cyber Horus group is known as a cybercriminal group offering its services to states, especially authoritarian states, this should also highlight how cyberwarfare between enemy states can be outsourced to independent contractors, in a similar manner in which private military contractors offer their services to states and rogue individuals. M. Aschmann, J Jansen and L. Leenen also argue about how non-state actors (independent hackers) launch cyber offensive and defensive operations, on behalf of clients which include governments, military forces or members of the private sector in exchange for financial remuneration (Aschmann, Jansen and Leenen 2015,18).

Ultimately, a more adequate term can be used to define state-backed cybercriminal groups, which can be that of 'cyber proxies', which are state-sponsored groups that aid the national objectives of a state and can be rather valuable in political warfare. Cyber proxies operate outside conventional war but within the sphere of influence of the state sponsoring them. This is done with the understanding that the conducted illegal activities will be tolerated as they support the national objectives of that nation-state. Another factor within the use of cyber proxies is that of plausible deniability. The nation-state that may be targeted by a cyber proxy might be able to attribute an attack to a specific sector, but they will encounter difficulty in ensuring that there might be an existing link between the actor and the nation-state sponsoring the attack. States within this scenario emerge as the figures pulling the strings behind the scenes within the cyber domain.

This cyber-attack took three days for the Ethiopian national cyber security team to disrupt, highlighting how Ethiopia in this scenario demonstrated at least some sort of cyber resilience. The strength of the prince is demonstrated, as Ethiopia manged to

gain access to its systems. In the aftermath of the cyber-attack as well, Ethiopia adopted a range of legislative and technical policies in the event of another cyber-attack. The saying that a good crisis should never be wasted indeed proved true in this case, as Ethiopia learned from the malware incident and adopted systems and mechanisms to ensure that such an attack in future can be better mitigated. This act of cyber coercion proved to be an act of state-backed cyber sabotage.

Almost a year later in April 2021, as a means of boosting capabilities to prevent and mitigate against cyber-attacks, Ethiopia unveiled a new headquarters allocated to the Ethiopian Information Network Agency to the value of 2.1 billion birr, which is around $40.4 million which is also equipped with advanced technological devices (Chandrakant 2022,171-172). This can be seen as Ethiopia pursuing/bolstering the strength of the prince by further capacitating their intelligence forces to adopt resilience measures aimed at cyber offence; ensuring the strength of the lion to ensure the survival of the Machiavellian prince.

Before the July 2020 cyber-attack, Ethiopia maintained membership in the Bilateral Alliance for Mutual Progress, which is a cooperation agreement aimed at bolstering the overall level of cyber security of members via the development of experiences and cyber trend sharing. The MoU between Israel and Ethiopia is also a multi-stakeholder agreement between members of Israel, Zambia, Ethiopia, Uganda, South Sudan, Rwanda, Kenya and Tanzania revolving around economic affairs and cyber security signed 5th July 2016. Ethiopia is also a member of the Common Market for Eastern and Southern Africa (COMESA) cyber security bill Model Bill, which entails the objective of harmonisation of cyber security policies, which also provides a roadmap for the adoption and implementation of cyber policies. Ethiopia is also a signatory of cyber security agreements with organisations such as the African Union, International Telecommunications Union and United Nations.

Local legislation such as the Computer Crime Proclamation No.958-2016, is more of a bill similar to South Africa's Cybercrimes Act of 2021, where the legislation defines and specifies penalties for computer crimes including crimes against computer systems and computer data; but notably crimes such as forgery, fraud and illegal content data. This piece of legislation makes almost no mention whatsoever of cyber crimes such as cyber espionage and cyber sabotage, hence, it proved a largely ineffective bill during the Egyptian cyber-attack on Ethiopian systems.

Ultimately, in the aftermath of the Egyptian act cyber-attack, Ethiopia adopted technical capacity as well -which entailed the creation of a Cyber Force Division, which was implemented on October 26th, 2022, shortly after the attack on critical systems, this was largely aimed at safeguarding national security and tackling vulnerability of cyber systems.

Under the guidance of the Federal Republic of Ethiopia, a new National Cyber Security Policy strategy was also unveiled, which was tasked with the duty of protecting national interest via capacity building and protecting the state's data and critical infrastructure, within this framework the 'Ethiopian Cyber Emerging Readiness and Response Team' Ethio-CERT was also implemented which was

mandated to create a secure, reliable and enabling Ethiopian cyberspace by coordinating and building national capacity. This is also a similar strategy compared to that of South Africa, where South Africa also made use of a Computer Systems Response Team, aimed at preventing cyber-attacks on Critical Infrastructure (CSIRT) under its NCPF framework.

It is worth highlighting that another variable that Ethiopia shares with South Africa, is the fact that at the time of the cyber-attack, Ethiopia also experienced a period of internal turmoil as a result of the Tigray conflict.

Case Study Three: Kenya

Cyber Espionage: Phishing

Hard to tell the good guys from the villains.

In mid-2022 after an extensive investigation, it was discovered that between 2019 and 2021, China via a cyber-proxy group known as 'BackDoorDiplomacy', employed the use of cyber espionage tactics as a means of covertly gathering sensitive information on the Kenyan state. At present Kenya is a major recipient of the Chinese Belt and Road Initiative, benefitting from a range of Chinese finance instruments such as development finance, investments and loans. The Chinese Digital Silk Road is another major source of digital development for the African continent, as well as several African states including Kenya.

Ultimately, several African states including Kenya have become exceptionally reliant on Chinese technologies as a means of leveraging technology for development, while this has brought with it advancements in internet connectivity, digital finance and the construction of digitally enhanced smart centres, this has also largely left Kenya exceptionally vulnerable to Chinese cyber spying. States that develop digital technologies may routinely and secretly design technologies in such a way that allows them the ability to collect intelligence and information from consumers of these technologies.

In line with China's state-centric regulation of technology firms including China's notion of digital sovereignty, whereby all technology firms are compelled by law to share data with the state; this is also a factor that in the long term may undermine the cyber security of several African states as consumers of Chinese technology. Willem

Gravett also highlights how Chinese firms are closely regulated to serve the strategic objectives of the Chinese Communist Party, and how Huawei was founded by Ren Zhengfei, a former officer in the military technology division of the 'People's Liberation Army', fostering strong ties between Huawei's management and the Chinese security and intelligence apparatus (Gravett 2020,131-132).

According to a cyber espionage report by the Kootneeti group, Chinese hackers conducted extensive covert cyber operations targeting key Kenyan ministries and governmental departments (Kootneeti Group 2022,1). These cyber espionage attempts seem to be closely linked to Kenya reportedly defaulting on Chinese loans. Ultimately, the Kootneeti Group also highlight how for a period spanning three years; Chinese hackers covertly targeted eight ministries, with the ministries of Foreign Affairs, Finance and even the Office of the Presidency affected, whereby intelligence documents were also illegally obtained (Kootneeti Group 2022,2).

Chinese hackers gained access to these classified flies via a spear-phishing attack when a government employee downloaded an infected file that essentially spread a virus to several critical systems; this was essentially a back door means for hackers to gain access to these protected files. According to the Kootneeti report China's hacking team referred to as 'BackDoorDiplomacy' was identified as the perpetrator, this is also the same cyber proxy with a history of furthering Chinese diplomatic objectives via cyber espionage operations and has previously targeted state institutions in Asia and Europe (Kootneeti 2022,2). This act of cyber espionage can be linked to China's desire to protect its economic and strategic interests abroad.

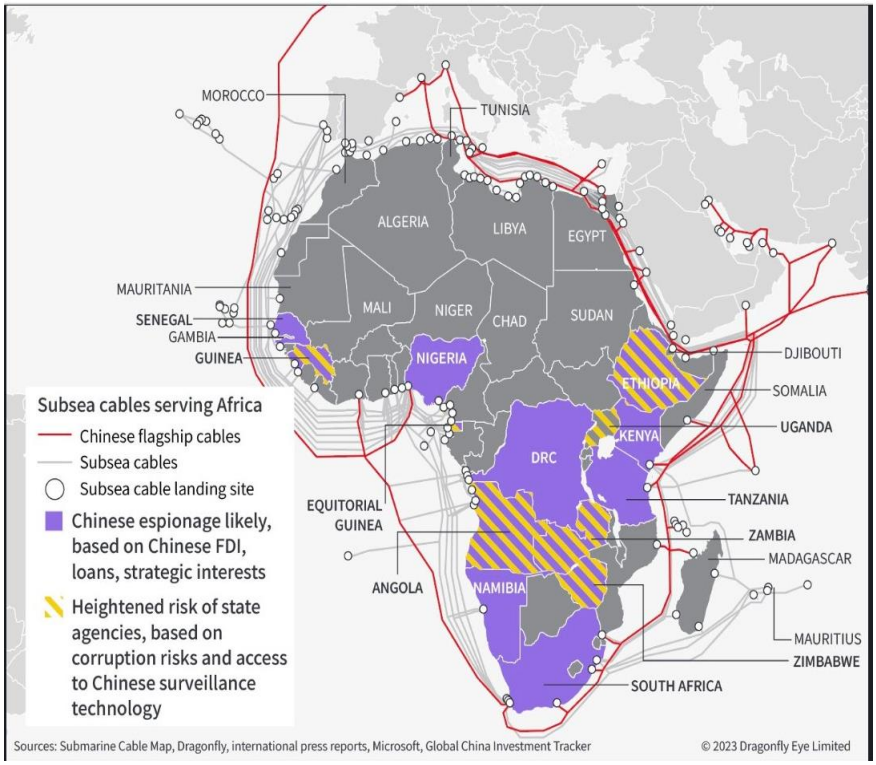
This is a failure on behalf of the Kenyan state and a major threat to the national security of the Kenyan state. For three years Kenya showed no situational awareness of this prolonged cyber espionage campaign. Ultimately, the national intelligence community demonstrated no characteristics of the 'Prince' as they could not launch and counter operations of cyber offence or defence; hence, Kenya was not as cunning as a fox or as fierce as a lion in thwarting this act of cyber espionage.

Kelli Vanderlee draws upon how Chinese cyber espionage operators use vulnerability exploitation, third-party compromise, and software supply chain compromise, as a means of gaining access to protected systems, files and data (Vanderlee 2022,2). This was precisely what 'BackDoorDiplomacy' did as they utilised vulnerability

exploitation to gain access to Kenyan documents and systems. China has also been guilty of using cyber power as part of its soft power strategy and as a means of spreading its influence, this an also another perfect example of how cyber operations are routinely employed in today's technological world whereby states can achieve their foreign policy objectives. Kenya in this case proved to be an unwilling participant and victim of Chinese cyber espionage. According to Zack Cooper, China's cyber operations form part of a web of complex and multipolar technology development strategy that employs licit as well as illicit methods to achieve its strategic objectives; currently, the Federal Bureau of Investigation estimates that China has more than 30 000 cyber spies, including an additional 150 000 private sector cyber experts (Cooper 2018,9-10).

Map two below gives a graphic depiction, showing Kenya, South Africa, Namibia, Nigeria and the Democratic Republic of Congo as being victims of Chinese cyber espionage.

Map 2



Source: Dragon Fly Intelligence: Chinese Espionage in African, 2023.

According to the Kenyan National Security Strategy of 2022, cyber strategy is based on six pillars namely, cyber governance, cyber security laws regulations and standards, critical information infrastructure protection, cyber security capability and capacity building, cyber risk and cybercrime management including cooperation and collaboration (National Cyber Security Strategy 2022,7-8). All these pillars are ultimately tasked with the core objective of safeguarding Kenya's critical information infrastructure.

Kenya also holds membership with the African Union Cyber Convention Group, International Telecommunications Union and UN Committee on Cyber Security. In November 2021, Kenya launched what would be known as the Computer and Cybercrimes Coordination Committee (NC4), which comprised of the Interior Cabinet Secretary, Ministry of Information, Ministry of Communication and Technology including the Inspector General of the National Police Service. Within the National Police Inspector General, a cybercrimes unit is tasked with investigating cybercrimes about fraud, technological means of financing terrorism and liaison with other states on international cybercrimes surrounding cross-border criminality.

Kenya also makes use of key legislation to safeguard their cyber domain, most notably the Computer Misuse and Cybercrimes Act of 2018; this act functions as a guide to combat computer misuse and cybercrime by facilitating investigation procedures for local and international cooperation. What is rather interesting within the context of this piece of legislation is that it goes into some detail defining and laying out what must be done in the event of an act of cyber espionage.

The Computer Misuse Crimes Act defines espionage as the activity of unlawfully and intentionally performing the prohibited activity of gaining access to either a critical database or national critical infrastructure, to intercept data, to, from, or within a critical database to directly benefit a foreign state against the Republic of Kenya (Computer Misuse Crimes Act 2018,56-58). Hence, one can see how both 'BackDoorDiplomacy' and China are in direct violation of the Computer Misuse Crimes Act of 2018, as China employed the services of 'BackDoorDiplomacy' with the objective of unlawfully and illegally gaining access to critical Kenyan information databases.

While this Computer Misuse Crimes Act does an adequate job of defining cyber espionage and laying out penalties for the activity, this act seems to be more effective when targeting a 'lone wolf attacker' as opposed to state-backed instances of cyber espionage and cyber sabotage. Tamas Gaidosch defines a lone wolf attacker as someone who engages in cyber-crimes such as phishing, espionage and sabotage for remuneration or as an act of hacktivism (Gaidosch 2018,3-4). The Computer Misuse Act even sets out penalties such as imprisonment and fines for individuals caught undertaking acts of cyber espionage (Computer Misuse Act Act 2018,58).

This Act proved exceptionally toothless against China's cyber espionage campaign against Kenya, the National Police Inspector General itself failed to counter the cyber espionage campaign nor did it even launch an investigation into the cyber incident; it was Kenyan cyber security experts that discovered and reported the attack. Two senior cyber security experts in an interview with Reuters journalists Aaron Ross, James Pearson and Christopher Bing, speak about how the attack resulted in key documents being stolen from the ministries of Foreign Affairs and Finance; the hack began in 2019 and ran up until mid-2022, cyber security analyst also points to how hackers secretly accessed an email server utilised by Kenya's National Intelligence Service (NIS), (Ross, Pearson and Bing 2023).

Ultimately, Kenya showed absolutely no resilience to this act of cyber espionage, both its ability to undertake campaigns of cyber offence and cyber defence was almost practically non-existent. If Kenya were a Machiavellian Prince, it would be a prince slayed to death by the enemy as Kenya in this scenario embodied no cunning cyber defence ability like the fox or cyber defence strength of the lion. The cyber incident of cyber espionage should highlight how dangerous it is to the national security of a state to be overly reliant on foreign technologies, as for one it keeps vulnerable to cyber-attacks and the weaponisation of cyber technology and two it undermines the state's ability to be the main custodian of security.

There is however a gripping question to be asked here, while Kenya has a strong national cyber strategy encompassing a cyber policy, structure, legal framework and cyber cooperation agreements, ensuring for the protection of critical infrastructure and national security. Did Kenya simply choose not to respond to the cyber incident purposefully? Initially, several senior Kenyan policymakers denied that the cyber

intrusion had even occurred, only later did senior Kenyan cyber officials and specialists admit that there has been a cyber intrusion of the Kenyan server. Hence, as a result of Kenya being a major benefactor of Chinese investment and trade including a key partner of the Chinese Belt and Road Initiative; did Kenya simply choose not to take action against 'BackDoorDiplomacy' as a policy decision aimed at avoiding confrontation with China, as any animosity between Kenya and China could potentially entail vastly negative consequences for the Kenyan economy. Kenya could have in this case chosen not to attribute the cyber incident to China, as once attribution is made members of the public largely expect some sort of action or response from the Kenyan government. Hence, in this case, Kenya could have chosen not to attribute the cyber espionage campaign to manage escalation risk.

The close link between economic forecast and the cyber domain must not be underestimated. Challenges within the cyber domain are connected, hence, solutions to cyber security and cyber incidents must be interconnected. Economic leverage coupled with cyber dependency could also be a hidden factor in how a weak state responds to a cyber incident by a powerful non-state actor backed by a state.

Making Sense of It All: What Picture Does Close Examination of These Cases Tell Us?

The most basic conclusion one could come to is that disruption does need planning if African states wish to pursue development using digital means and incorporating greater technologies as a means of better performing its functions as a state; cyber security must also be pursued as a means of safeguarding any of these systems from cyber incidents such as ransomware and malware.

While South Africa has pursued private-public partnerships to safeguard the cyber domain, greater forms of techplomacy must be pursued on the African continent. Cyber security is a function that cannot be reliant upon the state as the sole protector. The private sector has an important role to play, especially since most technological innovation occurs within the private sector, while cyber legislation is the priority of the state.

In the global North, many countries invest and safeguard in what is known as national pride industries and sectors. This is done to pursue national interests and safeguard national security. South Africa, Kenya and Ethiopia but Africa as a whole should be investing in technological innovation under a framework of continental national pride industry development projects aimed at driving homegrown cyber technologies; to safeguard a nation's national cyber security domain and be a competitive actor within the cyber realm.

Along with safeguarding existing critical information infrastructure, African states should also be equally as invested in developing new information infrastructure; as a means of strengthening the national security of the state. Bhaso Ndzendze and Tshilidzi Marwala, draw upon how infrastructure provides an interface between international relations and technology as it shapes patterns in regionalisation, national security thinking, foreign assistance and economic development (Ndzende and Marwala 2021,28-30).

Absa Bank has recently launched the ‘Absa Cybersecurity Academy’, to address the worldwide cyber security skills shortage; the programme also takes youth from marginalised backgrounds and trains them in the field of cyber security. Governments should be partnering with such organisations because such strategies achieve three goals of vital importance to state capacity. One, if it invests in local cyber skills, such individuals will one day be perfectly equipped to be the state’s main cyber warriors, while fostering close collaboration between the tech industry and the state: in essence a bolstering of techplomacy. A third factor ensures job creation as these marginalised youth are given purpose and an income. Partnership over isolation must be pursued as a means of safeguarding the cyber realm. While also keeping the central notion that states have a responsibility to cooperate on matters of national and international security. Cyber security is a matter of vital interest to both states and the international community as a whole, more especially as the globe must now learn to live within the age of artificial intelligence.

Classifying Cyber Incidents Affecting Kenya, South Africa and Ethiopia:

State	Cyber Incident/Attack	Cyber Tool
South Africa	Cyber Sabotage	Ransomware
Ethiopia	Cyber Sabotage	Malware
Kenya	Cyber espionage	Spear-phishing

Table Compiled by Student.

What is clear when examining the three selected cases is that the cyber incident tool employed by cyber attackers is usually intended to ensure a desired outcome. In cases where a cyber-criminal individual/group is interested in attaining a ransom for encrypted files and data such as in the Transnet attack; the method of preference would be a ransomware attack as opposed to a malware attack. The cyber tool employed in the wake of a cyber incident may serve as a good tool to an individual or law enforcement agency as a means of ascertaining as to what is the motive behind the cyber incident; and how to respond to it, either employing cyber defence or offensive strategy.

In the case of Kenya and South Africa, one can see how cyber incidents are closely linked to monetary or economic motivations as well; and how a cyber-attack on critical systems can very quickly become an economic problem as well. Hence, safeguarding the cyber domain is a key imperative as a means of safeguarding the state's economic prosperity and as a whole its national security. The ransomware attack on Transnet, resulted in macroeconomic shock as a result of a disruption to value chains, while the cyber espionage incident on Kenyan data systems was closely linked to Kenya defaulting on debt repayments. All these factors highlight how issues affecting the cyber domain are closely connected to economic and political factors; hence, when national security teams and political advisors devise a national cyber security policy; they should essentially bear in mind that cyber problems are connected, and solutions should be interconnected as a means of safeguarding both the cyber domain and economic prosperity of a state.

What also proved to be an interesting discovery as a potential factor capable of undermining the cyber resilience of both South Africa and Ethiopia; proved to be that of internal turmoil and political instability. Both acts of cyber sabotage that affected South Africa and Ethiopia coincided with internal conflicts such as the July Riots in

South Africa and the Tigray conflict in Ethiopia. During times of war and unrest, this notably puts additional pressure on security agencies as the goal then is to quell violence and return to law and order. Hence, law enforcement authorities in South Africa during this period were largely overwhelmed and caught off guard by the July Riots, which resulted in the deployment of the South African National Defence Force. It is then no surprise that cyber criminals seized upon this opportunity as South Africa's vulnerability then; translated into the crime being relatively easy and chances of being caught drastically decreased.

Ethiopia began construction of the GERD during the Arab Spring, a period when Egypt was at its weakest plagued by protest and instability and left unable to counter the construction of the GERD. Hence, when Ethiopia experienced a period of political instability as a result of the Tigray conflict, it was almost surprising to see the state hit with a cyber-attack during its period of uncertainty; it indeed seems as though Egypt repaid the favour or capitalised upon the opportunity of Ethiopian forces being unable to respond to the attack due to being over-stretched at that particular point in time.

The Ethiopian Information Network Security Administration (INSA), an institution launched in 2006 by the Ethiopian security cluster to build national cyber power capable of protecting national interest; seemly was itself caught napping as it had no intelligence or pre-emptive knowledge of the possibility of an incoming cyber-attack.

What is also a common factor shared by South Africa, Ethiopia and Kenya, is the fact that they were all reactive to cyber incidents/attacks as opposed to being proactive. Only after acts of malware, ransomware and cyber espionage did these states implement steps to increase cyber security detection and mitigation strategies. One crucial question that has to be raised is the fact that if these cyber incidents did not occur, whether or not South Africa, Ethiopia and Kenya would have more favourable cyber risk management strategies. Just as states conduct covert operations aimed at criminal and terrorist organisations intelligence gathering, African states should also be conducting covert operations aimed at identifying cyber actors on the continent and from which states is a cyber-attack likely to come.

Another issue to raise is the fact that upon closer investigation of these three states cyber legislation, is the fact that local legislation is aimed more toward cyber incidents/attacks emanating from within their borders; while this is exceptionally

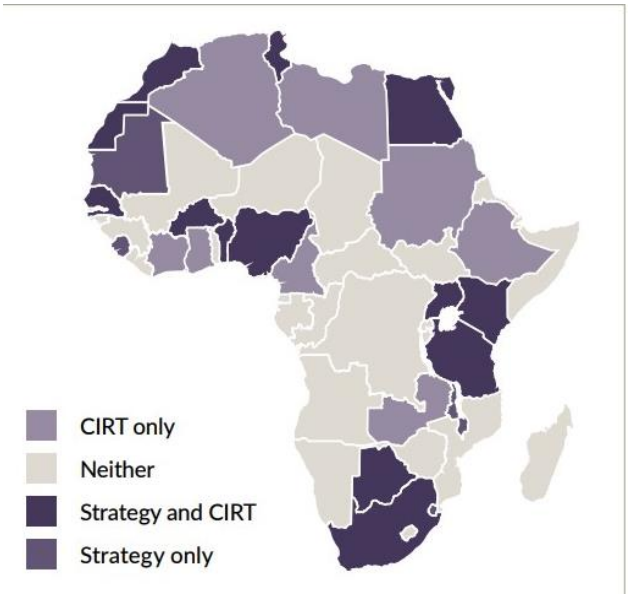
effective legislation when pursuing local lone wolf attackers and cyber criminals it proves to be toothless legislations in instances where these states are attacked by powerful cyber non-state actors and advanced cyber capable states. South Africa, Ethiopia and Kenya are also not signatories and have not even ratified the Malabo Agreement, a legislation aimed at developing a continental cyber norm and countering cyber-attacks from outside states and technologically advanced non-state actors. Without ratification of the Malabo Agreement, the cyber domain on the African continent but in these three states in particular remains weaker; for as Thucydides once said, 'the strong do what they want and the weak accept what they have to'. In essence, no ratification of the Malabo Agreement will see South Africa, Ethiopia and Kenya remain weak and accept what they have to from technologically advanced states and non-state actors.

African National Cybersecurity Strategies						
Country	Threat Assessment	Plan of Action	Timeline	Assignment of Responsibilities	Allocation of Resources	Last Updated
Benin	✓	✓		✓		2020
Burkina Faso		✓				2019
Egypt	✓	✓	✓			2018
Eswatini	✓	✓	✓	✓	✓	2020
Gambia		✓		✓		2016
Ghana		✓	✓	✓		2020
Kenya	✓	✓	✓	✓	✓	2014
Malawi		✓	✓	✓	✓	2017
Mauritius		✓	✓	✓		2014
Morocco		✓	✓	✓	✓	2013
Nigeria	✓	✓	✓	✓		2021
Rwanda		✓	✓	✓	✓	2015
Senegal	✓	✓	✓	✓	✓	2017
Sierra Leone	✓	✓	✓		✓	2017
South Africa		✓		✓		2012
Tanzania		✓		✓		2016
Uganda		✓				2014
TOTAL	7	17	11	13	7	

Source: African Center for Strategic Studies: African Lessons In Cyber Strategy 2022.

According to the above graph by the African Centre for Strategic Studies, Kenya and South Africa last updated their national cyber security strategies nearly a decade ago. This is exceptionally dangerous, especially in the wake of emerging technological advancements such as artificial intelligence that pose great risk and have even been defined by some experts as existential threats to states. This also highlights how

outdated South Africa and Kenya's strategies are, as these strategies are based upon the cyber landscape in 2012 and 2014 and reflect no preparedness for the current cyber threat landscape.



Source: Information Technology Union: Global Cyber Security Index 2022. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

As one closely interrogates the cyber security index map of Africa, what is disturbing is the fact that a large proportion of the continent has neither a cyber security strategy nor a computer incident response team. Africa is essentially a continent in a state of cyber vulnerability, and indirectly a haven for cyber-criminal organisations to both carry out attacks on the continent and upon other countries from the continent. The weaponisation of information as a result of mis and disinformation, cybercrimes acts of cyber sabotage and cyber espionage prove to be high-gain, low-risk activities in Africa.

Cyber security encompasses key pillars such as a cyber strategy being cyber legislation, technical capacity being cyber systems and human capital including response teams in the event of cyber incidents to mount acts of cyber defence and offence. The co-dependence and interconnectedness of these key pillars are what should ultimately attain the objective of safeguarding critical information systems. Yet, according to the cyber security index of the case studies used within this research

report only South Africa and Kenya have both a cyber strategy and computer incident response teams; while Ethiopia only has a computer response team to safeguard critical systems. This ultimately reveals that Ethiopia is lagging behind its African counterparts. What is also revealing is the fact that while Ethiopia is lagging behind the likes of South Africa and Kenya; Ethiopia seemed to have better thwarted the cyber-attack the state experienced by only employing their use of their technical skills capacity. This comes as Ethiopia disrupted the cyber espionage campaign after three days, while South Africa and Kenya took far longer than that when ensuring the integrity of their critical information systems.

What the cases of Kenya and Ethiopia also highlighted, and which may be subject to further study, is the fact that the cyber incidents that these states encountered were very closely linked to foreign policy objectives and geo-political conflicts as the cyber proxies that committed the incidents were at the time technologically advanced states that sought to achieve and safeguard their national interests within Ethiopia and Kenya. This should very well highlight that in an increasingly digitalised world, just as states employ wars, diplomacy and foreign investment to achieve and maintain their national interests; states are also more than willing to employ technology as a means of countering or destabilising competing states and actors.

The cases of Kenya and Ethiopia also imply that the technological revolution is increasingly setting the conditions for modern warfare, meaning that academics, policymakers and intelligence agencies must adjust perspectives when it comes to warfare, no longer is warfare solely conducted using guns, battle tanks and fighter jets-cyber warfare now features prominently in the military and foreign policy objectives of states as well. In the context of this research report but more especially when examining the cases of Kenya and Ethiopia, it can be seen as to how cyber security is a continuation of three different activities-which are rather old traditions, these traditions include sabotage, intelligence collection and subversion.

Conclusion:

Benefiting from the possible economic and developmental potential of technology has become part of the national interest of not just South Africa, Kenya and Ethiopia; but the entire African continent as a whole as African states, private sector and regional organisations as a whole have charged toward the increase adoption of various technologies. While this embracement of the technological revolution is a positive step, increased adoption without the adoption of cyber protection strategies and technical capacity; could potentially see South Africa, Ethiopia and Kenya, become more victims of the downside of the technological revolution as opposed to anything else. Disruptions such as wars, climate change and artificial intelligence are all core global issues that need planning; hence, adoption and development of cyber programmes need planning and investment as well.

The fact that in 2023 only 15 African states have ratified the Malabo Agreement, paints a stark picture of the level of importance African policymakers have attached to the cyber domain; to add to this not one African powerhouse state has ratified this agreement, essentially turning this important piece of continental legislation into a toothless piece of paper. Cyber security or rather insecurity is not just a continental issue but a global issue as a whole. Weaker regions such as the African continent, states and regional organisations might even have to pool sovereignty as a means of strengthening the cyber domain.

For South Africa, Ethiopia and Kenya, pooling sovereignty to safeguard critical infrastructures and the cyber domain is but the only manner in which to ensure synergy across their cyber domain. Pooling sovereignty could even assist these case study states in better pursuing factors such as CCBMs (Cyberspace Confidence Building Measures).

Moliehi Makumane argues that how to pursue CCBM, governments and civil society around the world must cooperate to advance cyber protection, CCBM's are critical as such systems enable dialogue between states in mitigating the destabilising effects posed within the cyber domain, while enabling mechanisms within the cyber domain (Makumane 2023,3). While Makumane makes a good point in stating that civil

society and governments must work together to foster information sharing and safeguarding the cyber domain; one could argue that South Africa, Ethiopia and Kenya, should also be employing an element of techplomacy here, as private sector organisations where technological innovation takes place must also be invited alongside governments and civil society organisations; this in essence will foster synergy between the legislators of technology and creators of technology; where all three parties play a critical role in protecting critical information systems. This ultimately ensures that South Africa, Kenya and Ethiopia will have both the cunning ability of the fox and the strength of the lion in ensuring that their critical information systems and technical capacity have the survival ability of a true Machiavellian Prince.

Moliehi Makumane also points out how CBMs can also be a source of empowerment for states; CBMs can be best rolled out through regional economic communities, where existing structures allow for easier information sharing; the most prominent CBMs include cooperative measures, transparency measures, inter-continental policy dialogues and lastly high-level visits to promote CBMs and multilateral CBMs; confidence building within this paradigm can be an iron blade for both cyber security and digital transformation; as digital trust, RECs as strategic partners and cyber stakeholders are all brought together under one umbrella (Makumane 2023,4-12).

Cyber Space Confidence Building measures are also important on both an internal and external level as well. Externally states should be pooling their sovereignty with regional economic communities/organisations; while internally South Africa, Kenya and Ethiopia, should also be working alongside citizens, the private sector and non-governmental organisations to bolster their cyber domain.

	E-Gov	Human Capital	E-Participation	Telecomms Infrastructure
SA	Rank-65 Value:0.7357	Value-0.7733	Rank-61 Value:0.5909	Value:0.6850
Ken	Rank-113 Value:0.5589	Value:0.5641	Rank-64 Value:0.5795	Value:0.4305
Eth	Rank-179 Value:0.2865	Value:0.3364	Rank-163 Value: 0.1932	Value:0.1501

Table: Compiled By Student

Data source: https://publicadministration.un.org/egovkb/en-us/Data-Center

Looking at the United Nations E-Governance Index, it is strikingly visible that Ethiopia, Kenya and South Africa, require much more capacity and investment in key sectors as a means of safeguarding their cyber domain. To start in Ethiopia and Kenya much more investment is needed in human capital, as a means of ensuring that more cyber skills amongst their respective populations are garnered. In terms of fostering greater levels of e-participation South Africa and Kenya are just about touching the midpoint, while Ethiopia is way behind in driving greater levels of e-participation. Ensuring that more citizens have access to the internet is critical, as the Internet today is a source of knowledge and training. The garnering of knowledge and training is of utmost importance if this case states both want to raise awareness about cyber security, foster cyber skills and technical capacity and also maximise upon the potential economic benefits of technological advancements in the world of e-commerce.

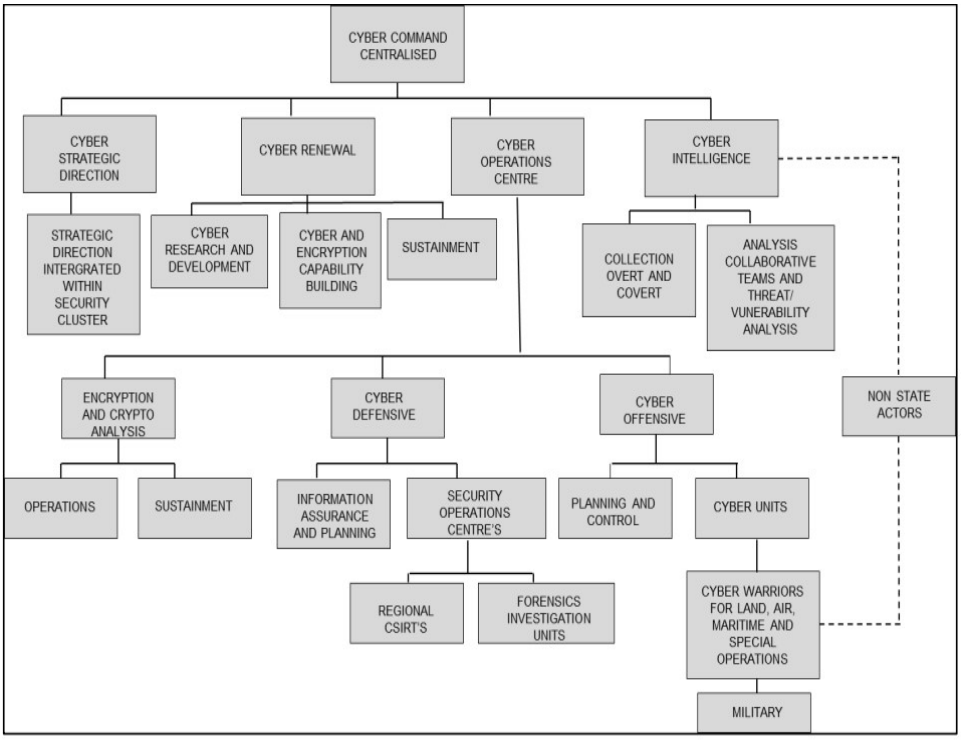
Armed forces part of South Africa, Kenya and Ethiopia's defence strategy routinely part-take in military drills, exercises and wargaming; as part of effectively ensuring combat readiness. Kenya and South Africa in 2023 alone have taken part in military drills alongside armed forces from France, Russia, China and the United States. Ultimately, just as wargaming and military drills form a key part of defence functions within the physical domain, wargaming must be undertaken within the cyber domain. Wargaming within the cyber domain can take the form of ethical hacking; to test the cyber offence and cyber defence capabilities of a state's cyber security capabilities. Wargaming within the cyber domain is capable of in fact strengthening cyber security, as cyber experts may be better able to identify system vulnerabilities, threats and possible responses to different types of cyber incidents. Possible scenarios may also be mapped out as a means of ensuring that all cyber systems can both prevent and mitigate cyber threats and challenges within cyberspace.

Another capability that could bolster national security against acts of cyber espionage and cyber sabotage, could entail the creation of cyber armies; these armies could add to military capability and form part of an unseen military capability of South Africa, Ethiopia and Kenya. Military forces perform the task of protecting the sovereignty and integrity of a state, including its civil society against a hostile state or non-state

actor; whose intentions are malevolent. Cyber armies in essence would perform the same functions as a military force but within the cyber domain as opposed to the physical realm; cyber armies ultimately, protect the sovereignty and integrity of a state's cyber domain.

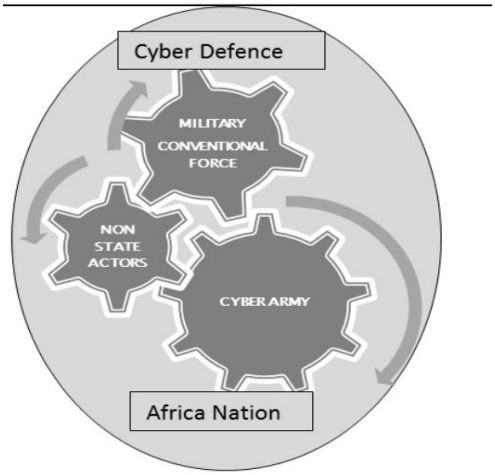
An African cyber army would in essence be a strategic asset and an added intelligence component for South Africa, Ethiopia and Kenya. As information in the digital industrial economic age is believed to be a strategic resource, hence, states are compelled to see protecting such information as a national security objective. The notion of an African cyber army would perform the function of both cyber offence and cyber defence. Michael Aschmann, Joey Jansen van Vuuren and Louise Leenen argue how the cyber defence task of a cyber army includes ensuring that military and government computer networks are secured and protected from both internal and external threats; while the cyber offensive task of a cyber army ranges between proactive and reactive launch of cyber-attacks using cyber means against adversaries aimed at, destroying, exploiting, corrupting or collecting information for intelligence purposes (Aschmann, Vuuren and Leenen 2015,3-4).

Ultimately it can be seen as to how a cyber army would add to the strength of the Machiavellian Prince, as it entails both the characteristics of the fox and the strength of a lion; to both evade and launch cyber-attacks. A cyber army is broadly described as an unseen strength of a military. Micharl Aschmann, Joey Jansen van Vuuren and Lousie Leenen highlight how the core functions of an 'African Cyber Army' include the establishment of a centralised cyber command capability, the ability to research and develop within the cyber environment, building offensive and defensive cyber capabilities, execute encryption and crypto analysis, including that of employing and training of cyber warriors (Aschmann, Vuuren and Leenen 2015,8-9).



Proposed structure of African cyber army.

Source: Cyber Armies: The unseen military in the grid 2015.



Source: Cyber Armies: The unseen military in the grid 2015.

While a cyber army might be feasible for states such as South Africa, Egypt and Nigeria; it is largely unfeasible to many other African states such as Kenya and Ethiopia. Cyber skills are also very scarce on the continent, located in pockets of the continent, mostly in South Africa, Nigeria and Egypt. Hence, the scarcity of resources to fund a cyber army and a shortage of cyber skills in states leaves the idea of a cyber army unattainable to many.

The protection of information systems, data, and critical infrastructures remains a shared imperative to many in Africa, hence, the creation of regional cyber armies might be more attainable for the likes of Ethiopia and Kenya; where regional communities such as the East African Community and Common Market for East and Southern Africa, may form the hubs for the creation of regional cyber armies. Organisations lower transaction costs and pool expertise, hence, in circumstances where cyber skills are scarce and finances are slim such as in the case of Ethiopia and Kenya, and even to some extent South Africa; regional organisations might be the best bet to form regional cyber armies where expertise is pooled. This may even be better than having cyber armies at a state level as regional cyber armies may better facilitate information gathering and sharing, while acting as forces that better foster cyber norms and standard setting in these regions.

This was an exceptionally rewarding study to undertake, given the age of technological advancement and artificial intelligence domain that the world now finds itself in. Due to this study being part of the requirements of a master's programme, I believe that it could be expanded with a bit more resources in the future. The research could have been made slightly richer in content if travel to these case study states was allowed, as a means of undertaking interviews with relevant policymakers and listening to those personally affected by the Ethiopian cyber incident. Factoring in personal accounts of private sector corporate leaders who had been affected by the Transnet cyber sabotage attempt would have also added a unique richness to the research. As mentioned earlier in the report the ransomware incident caused a macroeconomic shock, which cost the entire SADC regional economy 9 billion Dollars. Ultimately, it would have been fruitful to speak to private sector businesses as a means of calculating the financial impact that the ransomware attack had on the private sector. Raw materials and tradable shocks are frequently transported by private sector businesses using the services of Transnet, hence, the impact the cyber incident had on both the private and public sector financial streams would have been good to measure as a means of determining which sector proved to be more resilient to the shock and was able to recover quicker.

Upon reading this research report a notable question that might arise could be what future/further research could be undertaken to add to this master's report. One could

argue that in the case of the Egyptian cyber-warfare campaign against Ethiopia; and the Chinese cyber espionage incident against Ethiopia, both the perpetrators used cyber tools as a means of pursuing their national interest. Hence, alongside traditional foreign policy tools such as coercive diplomacy, war, and economic coercion, cyber-attacks seem to have become new effective means of a state pursuing its national objectives. Ultimately, further research could entail, how have cyber tools become a new tool for states to utilise to further/safeguard their national interest. A study such as this could also help states and organisations across the globe better implement national security strategies that could safeguard their national systems during times of instability and conflict.

Total Word Count: 20 664

Bibliography

Albert Mathias and Barry Buzan. 2011. “Securitization, sectors and functional differentiation.” *PRIO* 413-425.

Allen, Karen. 2023. *On cybersecurity in Africa: Building critical governance partnerships.* Policy Brief, Stellenboach: Security Institute for Governance and Leadership in Africa .

Araujo, Laurent Celerier and Jose. 2023. *Research-driven Insights to Build A Safer Digital Society* . Research Report, Utrecht: Orange Cyberdefense .

Baron, Hans. 1961. “Machiavelli: The Republican Citizen and the Author of 'the Prince'.” *The English Historical Review* 217-253.

Center for Strategic and International Studies. 2022. *Significant Cyber Incidents Since 2006.* Washington: Center for Strategic and International Studies .

Claudia Pahl-Wostl, Xavier Basurto, Sergio Villamayor-Tomas. 2021. *Comparative case study analysis.* Barcelona: Routledge.

Collier, David. 2011. “Understanding Process Tracing.” *American Political Science Association* 823-830.

Danish Ministry of Foreign Affairs. 2018. *Techplomacy: How Denmark is Prototyping Foreign Policy.* Copenhagen : Denmark Ministry of Foreign Affairs.

Department of Communications. 2009. *Cyber Security Policy of South Africa.* Pretoria: Department of Communications.

Eboibi, Felix E. 2020. “Concerns of Cyber Criminality in South Africa, Ghana, Ethiopia and Nigeria: Rethinking Cybercrime and Institutional Accountability .” *Commonwealth Law Bulletin* 78-109.

Fabio Christiano, Xymena Kurowska and Dennis Broedev. 2024. “Cybersecurity and the politics of knowledge production: towards a reflexive practice.” *Journal of Cyber Policy* 1-33.

Gebreluel, Goitom. 2014. “Ethiopia's Grand Renaissance Dam: Ending Africa's Oldest Geopolitical Rivalry?” *The Washington Quarterly* 25-37.

Goodrick, Delwyn. 2014. *Comparative Case Studies.* Brief, Florence: Unicef.

Gravett, William. 2020. “Digital neo-Colonialism:The Chinese model of Internet Sovereignty in Africa.” *African Human Rights Law Journal* 125-146.

Guro, Ayele. 2020. *An emerging threat to Ethiopia’s national security the case of cybersecurity.* MA Report, Addis Ababa : Arba Minch University .

Hendrick Zwarts, Jaco Du Toit and Basis Von Solms. 2022. “A Cyber Diplomacy and Cybersecurity Awareness Framework (CDAF) for Developing Countries .” *21st European Conference on Cyberwarfare and Security.* Chester : Academic Conferences and Publishing International Ltd. 331-3349.

Ifeanyi-Ajufo, Nnenna. 2023. “ Cyber governance in Africa: at the crossroads of politics, sovereignty and cooperation.” *Policy Design and Practice* 146-159.

Information Regulator of South Africa. 2023. “inforregulator.org.za.” *Information Regulator South Africa.* 04 July. Accessed August 3rd, 2023. https://inforegulator.org.za/wp-content/uploads/2020/07/MEDIA-STATEMENT-INFRINGEMENT-NOTICE-ISSUED-TO-THE-DEPARTMENT-OF-JUSTICE-AND-CONSTITUTIONAL.pdf.

Interpol . 2021. *African Cyber Threat Assessment Report.* Lyon: Interpol.

International Monetary Fund. 2022. *Cybersecurity Risk Supervision and Oversight* . Washington: International Monetary Fund

Isletmesi, Iktisadi. 2020. “20 Years of Securization .” *Uluslararasi IIiskiler Konsey* 3-20.

Jamieson, Kathleen Hall. 2019. *How Russian Hackers and Trolls Exploited U.S Media in 2016.* Pennsylvania: Annenberg Policy Centre

Jansson, Per. 2018 . “Smartness as prudence: smart power and classical realism.” *Journal of Political Power* 341-358.

Jarrín, Shaun Riordan & Mario Torres. 2020. *GLOBAL POLICY PERSPECTIVE REPORT Techplomacy and the Tech Ambassador.* Brussels: European Institute of International Affairs.

Julia Voo, Irfan Heman, Simon Jones, Dan Cassidy and Anina Schwarzenbach. 2020. *National Cyber Index 2020.* Research Report, Cambridge : Belfer Center for Science and International Affairs.

Kasembeli, Brigid Gesami and Gregory. 2022. “Combating Cybersecurity Threats in the African Maritime Domain.” *Social Science Research Network* 8-16.

Kenyan Parliament. 2018. “Kenya Law.” *Kenya Law.* 30 May. Accessed June 25, 2023. http://www.kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/ComputerMisuseandCybercrimesActNo5of2018.pdf.

Koibi, Brian Njama. 2015. *Cybersecurity As an Emerging Threat to Kenya's National Security.* MA Report, Pretoria: University of Pretoria .

Kootneeti Group. 2022. *Chinese Hackers Target Kenya's Government in Long-Term Government Espionage Campaign.* Uttar: Kootneeti Group.

Kranzberg, Melvin. 1964. *Technology and Human Values.* Virginia: Virginia Quarterly Review

Lee Kuan Yew School of Public Policy. 2017. *Shaping Techplomacy through shifting sands in the global technological landscape.* Singapore: Lee Kuan Yew School of Public Policy .

Leffler, Melvyn P. 1990. “National Security.” *Journal of American History* 143–152.

Letseka, Grace Tabea. 2022. *Cybersecurity readiness in South African Public Sector Organisations.* MA Report , Johannesburg: University of Johannesburg.

Liquid Cloud . 2022. *Liquid C2 Cyber Security Report reveals that cyber attacks increased in Kenya, South Africa and Zambia by 76% in 2022.* London: Liquid Cloud.

Makoma Makhopa, Wellington Sikuka, Dirk Esterhuizen, and Katherine Woody. 2021. *Cyber-Attack Cripples Operations at the Port of Durban for Second Time In A Month.* Voluntary Report , Pretoria : Global Agricultural Information Network.

Marwala, Bhaso Ndzendze and Tshilidzi. 2021. *Artificial Intelligence and Emerging Technologies in International Relations.* Johannesburg: World Scientific .

Mbanaso, Uche M. 2016. “Cyber Warfare: African Research Must Address Emerging Reality.” *African Journal of Information and Communication* 181-210.

Mbembe, Achille. 1990. “Africa in Theory.” *Anthropological Quarterly.*

Mckenzie, Timothy M. 2017. *Is Cyber Deterrence Possibele?* Alabama: Air Force Research Institute Perspectives on Cyber Power .

Michael Aschmann, Joey Jansen van Vuuren,, Louise Leenen. 2015. *Cyber Armies: The Unseen Military In The Grid* . Cape Town: University of Western Cape .

Mutua, Grecie Sebina and Amy. 2023. *Civic Tech in Southern Africa: Alternative Democracy and Governance Futures?* Johannesburg: South African Institute of International Affairs.

Mzyece, Mzukisi Qobo and Mjumo. 2023. “Geopolitics, technology wars and global supply chains: Implications for Africa.” *South African Journal of International Affairs* 29-46.
Nate Allen, Matthew La Lime, Tomslin Nlar. 2022. *The Downsides of Digital Revolution: Confronting Africa’s evolving cyber threats.* New York: GI-TOC.
Ndeapo Wolf, Deon Cloete and Jan Hofmeyer. 2022. *SADC Futures of Digital Geopolitics: Towards African digital sovereignty.* Johannesburg: South African Institute of International Affairs .
Niekerk, Brett van. 2023. “Vulnerability of South African Commodity Value Chains to Cyber Incidents.” *Scientia Militaria* 161-186.
Nye, Joseph. 2010. *Cyber Power* . Research Report, Cambridge : Belfer Center for Science and International Affairs .
Olumide Abimbola, Faten Aggad , Bhaso Ndzendze. 2021. *What is Africa's Digital Agenda?* Berlin: African Policy Research Institute .
Pantserev, Konstantin A. 2022. “Malicious Use of Artificial Intelligence in Sub-Saharan Africa: Challenges for Pan-African Cybersecurity.” *Peoples’ Friendship University of Russia (RUDN University)* 288-302.
Patcharaporn Leepipatpiboon, Chiara Castrovillari, and Tomohide Mineyama. 2023. *Macroeconomic Shocks and Conflict.* Working Report, Washington: International Monetary Fund .
Petrus Duvenage, Wilhelm Bernahardt and Sebastian von Solms. 2022. “Cyber Power in the African Context An Exploratory Analysis and Proposition .” *22nd European Conference on Cyberwarfare and Security.* Piraeus: Academic Conferences and Publishing International Ltd. 177-186.
Reva, Deny. 2010. *South Africa's maritime domain awareness A capability baseline assessment.* Pretoria : Institute for Security Studies .
Roumate, Fatima. 2021. *Artificial Intelligence and Digital Diplomacy Challenges and Opportunities* . New York: Springer .
Sambuli, Iginio Gagliardone and Nanjira. 2015. *Cyber Security and Cyber Resilience in East Africa.* London: Chatham House .
Samme-Nlar, Tomslin. 2020. “The Future of Armed Conflict in Africa : What Cyber Attacks on Ethiopian Government Tells Us.” *Social Science Research Network* 61-71.
Scobell, Andrew. 2003. *China's Use of Military Force Beyond the Great Wall and the Long March.* Kentucky: Cambridge University Press.
Sekgololo, Mancha Johannes. 2021. *The State of Cybersecurity in South Africa, 2010-2019.* MA Report, Johannesburg: University of Johannesburg.
S. El Attar, Y. Rafaat & M. Mohamed. 2015. “Water Resources Management in Egypt.” *Journal of Engineering Scieneces* 269-279.
Sime, Tefesehet Hailu. 2023. “A Critical Reflection on African Maritime on African
Maritime Cybersecurity Frameworks.” *Scientia Militaria* 1-88.
Solms, PC Duvenage and SH Vin. 2015. “Cyber Counterintelligence: Back to the Future .” *Journal of Information Warfare* 42-56.
State Security Agency. 2015. *State Security and the JCPS* . Government Gazaette, Cape Town: Parliament of South Africa.
Suri, Anirudh. 2022. *The Great Tech Game* . Dheli : Harper Collins India.
Sutherland, Ewan. 2017. “Governance of Cybersecurity – The Case of South Africa.” *The African Journal of Information and Communication* 83-112.
Taureck, Rita. 2006. “Securitization theory and securitization studies.” *Journal of International Relations and Development* 53-61.

The Presidency . 2002. *ELECTRONIC COMMUNICATIONS ACT* . Cape Town: Parliament of South Africa.
Transnet. 2021. *Transnet Integrated Report 2021*. Integrated Report, Pretoria: Transnet.
United Nations. 2023. *UN New Agenda For Peace*. Policy Brief, New York: United Nations.
Walker, Summer. 2023 . *Still Polls Apart UN Cyber Crime Treaty Negotiations* . Policy Brief, New York: GI-TOC.
Ziemer, Tim Hall and Ulrike. 2023. "Exploring the relationship between IT development, poverty and cybercrime: an Armenia case study." *Journal of Cyber Policy* 121-134.