# Cyber Warfare

*Jabu Mtsweni and Mphahlela Thaba*

## Introduction

The African battlespace is rapidly changing, driven among others by several socio-economic factors. These factors in turn create a more complex, unpredictable, and volatile operating environment for African armed forces. The evolution of technology is forcing African governments to modernise the delivery of services through digital means, which in turn opens the door for multi-dimensional vector attacks. This has also led to the proliferation of advanced weapons, as well as the increasing use of information and communications technologies (ICT) in warfare, making it easier for non-state actors to wage asymmetric war and carry out terrorist attacks. The African cyberspace faces increasing cyber threats and several cyber incidents have been observed at government levels including attacks on militaries and sovereignty of Africa countries through election attacks, critical information infrastructure attacks, and cyber-terrorism. The loss of huge financial resources in Africa due to cyber-crime is also widely reported in the academic and business space. Moreover, state actors and non-state actors are increasingly targeting African states using cyber weapons. Therefore, the dominance of the cyberspace even for African militaries implies the need to be prepared to operate in this unfamiliar environment to maintain their security and stability. African militaries need to therefore develop new capabilities, especially in terms of cyber defence, to meet the emerging ICT challenges and multi-dimensional threats on the continent.

This chapter, therefor, discusses how African militaries and nation-states could systematically establish and deploy new cyber warfare capabilities to the modern battlespace. It begins by outlining the challenges that Africa faces in the cyber domain, including a lack of resources, expertise, and infrastructure. It then discusses how African nation-states have responded to these challenges at the distinct levels of warfare. The chapter covers four case studies comprising four countries in Egypt, Nigeria, South Africa, and Kenya. The case studies analyse the publicly available information on selected nation's threat landscape, capabilities, strategies, challenges, including regional and international cooperation by using the POSTEDFIT model. It also discusses the implications of the findings for African armed forces. In conclusion the chapter argues that

African armed forces need to continue to invest in cyber warfare capabilities to play a competitive role in the global cyber space.

**Background**

The African battlespace is undergoing rapid transformation driven by a confluence of socio-economic factors[1]. These factors have contributed to a more complex, unpredictable, and volatile battlefield for African militaries. The evolution of technology has compelled African governments to modernise service delivery through digital means, simultaneously exposing them to multi-dimensional vector attacks[2]. This has also led to the proliferation of advanced weapons and the increasing integration of ICT in warfare, facilitating asymmetric warfare, terrorist attacks by non-state actors, and covert cyber operations in Africa[3]. The pervasive influence of cyberspace, even for African militaries, underscores the need to adapt to this unique environment to maintain security and stability.

African militaries face a multitude of challenges in the cyber domain, including a dearth of resources, expertise, and infrastructure. These limitations hinder their ability to effectively participate in the cyber domain to defend against cyberattacks, ensure national security in the cyber space, utilise ICT to enhance operational capabilities, and exploit the cyber space for nations strategic objectives[1].The chapter uses a case study approach to study four African countries to explore their cyber warfare capabilities inclusive of challenges, international cooperation, and overall threat landscape. This is done by employing the POSTEDFIT model to comprehensively analyse the unique characteristics of each African nations' cyber warfare posture in Africa. The findings of the case studies have significant implications on cyber warfare capabilities development across the continent. The analysis of the case studies highlights the need for militaries to prioritise cyber warfare investments, strengthen international cooperation, and develop tailored cyber strategies to address the evolving threat landscape.

---

[1] Jabu Mtsweni and Mphahlela Thaba, 'Building an Integrated Cyber Defence Capability for African Missions,' *Journal of Information Warfare* 21(1) (2021): pp. 17-34.
[2] Thaba Mphahlela and Jabu Mtsweni, 'Developing Robust Cyber Warfare Capabilities for the African Battlespace,' *22nd European Conference on Cyber Warfare and Security (ECCWS 2023)*, June 2023.
[3] Jan Kallberg and Steven Rowlen, 2014, 'African nations as proxies in covert cyber operations', *African Security Review.* 23(3) (2014): pp. 307-311.

## Definitions and Context

The arena of the cyberspace is highly diverse with different terminologies, interpretations, positions[4], and capabilities focusing on cyber defence and/or attacks.

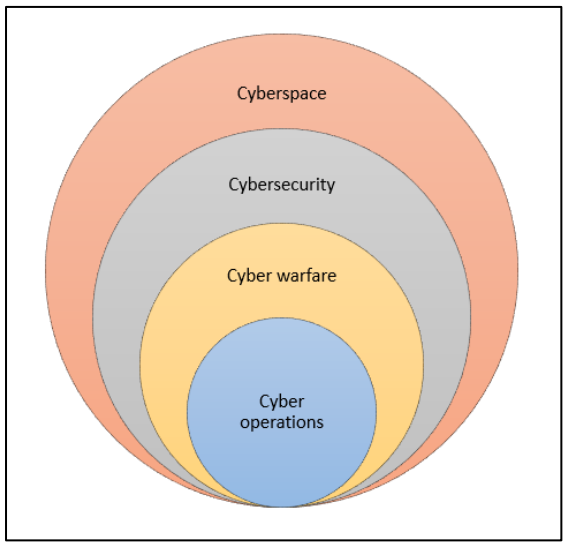


Figure 1: Cyber Warfare Context[5]

As depicted in **Error! Reference source not found.**, cyberspace is a domain of operation and is simply defined as a "*A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers*"[6]. In the military context, it is classified as the fifth operational domain of warfare and interacts with other domains of warfare such as space, air, land, and sea[4]. The understanding of this operational environment influences how nation-states including African military forces could build capabilities for securing and exploiting the cyberspace for the objectives. The understanding of this operational environment influences how nation-states including African military forces could build capabilities for securing and exploiting the cyberspace for the objectives.

[4] Daniel Hughes and Andrew Colarik, 'The Hierarchy of Cyber War Definitions,' in *Intelligence and Security Informatics,* edited by G. Waag, M. Chau and H. Chens (Cham: Springer, April 2017).
[5] Thaba Mphahlela and Jabu Mtsweni, 'Developing Robust Cyber Warfare Capabilities for the African Battlespace,' *22nd European Conference on Cyber Warfare and Security (ECCWS 2023)*, June 2023.
[6] NIST, 'Computer Security Resource Centre (CSRC)', Gaithersburg: National Institute of Standards and Technology, (2023).

While the terms war, conflict, and warfare are frequently used interchangeably, they hold distinct meanings. *War* is defined as an armed conflict between countries or groups aimed at overpowering one another[7]. In the cyber domain, war manifests as sustained and widespread cyberattacks between nations, capable of inflicting substantial damage to critical infrastructure or assets, causing loss of life, or triggering other severe consequences. *Conflict*, a broader concept, encompasses any disagreement or dispute between individuals, groups, or nations. In cyberspace, conflict manifests in a wide range of activities or actions committed by actors on an entity through different events[8] from low-level cyberattacks like phishing scams to sophisticated attacks targeting critical infrastructure. *Warfare*, a broader term than war, encompasses all aspects of war, including planning, preparation, execution, and aftermath. In cyberspace, *warfare* encompasses all activities undertaken by nations and other actors to prepare for, defend against, or carry out cyberattacks[9]. This includes activities like developing cyberweapons, training cyber warriors, and conducting cyber espionage.

*Cyber operations* are critical in every phase of the modern warfare and are in this chapter loosely defined as non-lethal elements of warfighting functions in the cyberspace that produce specific effect on a target, such as deny, disrupt, and destroy[10]. In practice, the lines between war, warfare, and conflict in the cyber domain can be blurred. For example, a cyberattack that causes considerable damage to critical infrastructure could be considered an act of war, even if it is not part of a wider armed conflict. And a low-level cyberattack that is part of a wider geopolitical rivalry could be considered an act of warfare, even if it does not cause considerable damage. In practice, the lines between war, warfare, and conflict in the cyber domain can be blurred. For example, a cyberattack that causes considerable damage to critical infrastructure could be considered an act of war, even if it is not part of a wider armed conflict. And a low-level cyberattack that is part of a wider geopolitical rivalry could be considered an act of warfare, even

---

[7] Radu Antonio Serrano Iova and Tomoe Watashiba, 'NCSS: A Global Census of National Positions on Conflict, Neutrality and Cooperation' *Proceedings of the 22nd European Conference on Cyber Warfare and Security (ECCWS 2023),* (June 2023).

[8] Scott Applegate and Angelos Stavrou, 'Towards a cyber conflict taxonomy', *In the 5th International Conference on Cyber Conflict,* (June 2013).

[9] Thaba Mphahlela and Jabu Mtsweni, 'Developing Robust Cyber Warfare Capabilities for the African Battlespace,' *22nd European Conference on Cyber Warfare and Security (ECCWS 2023)*, June 2023.

[10] Lt Col Arun Shankar, 'Offensive Cyberspace Operations: using artificial intelligence and kill chains to analyze the effects of MAGTF execution authority', Marine Corps Gazette, 24 January 2023, https://www.hoover.org/sites/default/files/research/docs/Offensive%20Cyberspace%20Operations%20-%20MCG%20-%20Feb%202023%5B93%5D.pdf, Accessed 18 January 2024.

if it does not cause considerable damage. As a result, the distinction between war, warfare, and conflict in the cyber domain is a matter of degree. The severity of the attack, the intentions of the attacker, and the response of the victim all play a role in determining whether a cyberattack is considered war, warfare, or conflict. In this chapter, our focus is more on the warfare aspects as these pertain to the whole cyber warfare capability development lifecycle, which is operationalised in peace and war times.

**Evolution of Warfare**

Warfare have evolved significantly over time, incorporating various technological advancements and strategic shifts. The emergence of computers in warfare can be traced to the late 1940s and early 1950s. This period marked the emergence of the initial stages of cyberwarfare, during and after World War II. Early computers were used for code-breaking and cryptographic purposes, laying the groundwork for the importance of information security in military operations[11]. Figure *2* below depicts the evolution of the concept of war over time, in generations.

| 1. Phase | 2. Phase | 3. Phase | 4. Phase | 5. Phase |
|---|---|---|---|---|
| Wars before nation-states | **1. Generation war** Classic wars (1648- 1830) Top point: Napolyon Wars | **2. Generation war** All together Industry Wars (1830-1918) Top point: I. World War | **3. Generation war** Maneuver Wars (1918-1948) Top point:1991 Gulf War | **4. Generation war** Unconventional Wars (From 1948 to our day especially aftermath of 11 September), Top point: US Afghanistan and Iraq Occupations. |

Figure 2: The Evolution of the Concept of War over time[12]

The 1970s and the 1980s saw the development of computer networks and communication. This signalled the emergence of the Internet which opened new avenues for military communication and intelligence gathering in military operations[12]. This period saw the military's increasing

[11] Claire H. Oakes and Kevin H Govern, 'Introduction: Cyber and the changing face of war', https://scholarship.law.upenn.edu/faculty_scholarship, accessed 28 November 2023.
[12] Huseyin Kuru, 'Evolution of war and cyber-attacks in the concept of conventional warfare,' *Journal of Learning and Teaching in Digital Age*, 3(1), (2018): pp. 12-20.

reliance on interconnected systems, making them susceptible to cyber threats[13]. In the 1990, militaries began to formally recognise information warfare as a concept within military doctrine. Militaries started to acknowledge the significance of information dominance, encompassing electronic warfare, psychological operations, and cyber activities. Information warfare was employed more during the Persian Gulf War, marking the importance of information warfare in modern conflicts[14].

In the 21st century, the world saw a rapid increase in the development and deployment of cyber capabilities by nations in what was termed the fourth-generation warfare[15]. Many militaries started investing heavily in offensive and defensive cyber capabilities, recognising the potential for cyber operations to influence geopolitical dynamics and military outcomes[16]. The evolution of the elements of cyberwarfare was marked by the discovery of Stuxnet in 2010 as shown in Figure *3* below. This was a sophisticated cyber weapon designed to target Iran's nuclear program, highlighting the potential for cyber-attacks to cause physical damage to critical infrastructure. This incident underscored the need for effective cyber defences and established a precedent for the use of cyber tools in state-sponsored operations[17].

[13] John Naughton, 'The evolution of the Internet: from military experiment to general purpose technology,' *Journal of Cyber Policy*, 1(1), (2016): pp. 5-28.
[14] Mica R Endsley and William M. Jones. *Situation awareness, information dominance, and information warfare.,* (United States Air Force Armstrong Laboratory: Wright-Patterson AFB, 1997).
[15] Huseyin Kuru, 'Evolution of war and cyber-attacks in the concept of conventional warfare,' *Journal of Learning and Teaching in Digital Age*, 3(1), (2018): pp. 12-20.
[16] Grace B Mueller, Benjamin Jensen, Bandon Valeriano, Ryan C. Maness, and Jose Macias, *Cyber operations during Russo-Ukrainian war: from strange patterns to alternative futures,* (Washington, United States, Center for Strategic & International Studies, 2017).
[17] Marie Baezner and Patrice Robin. 'Cyber defense hotspot analysis: Stuxnet', *Center for Security Studies,* October 2017, https://graquantum.com/a-brief-history-of-cyberwarfare/, accessed 18 January 2024.

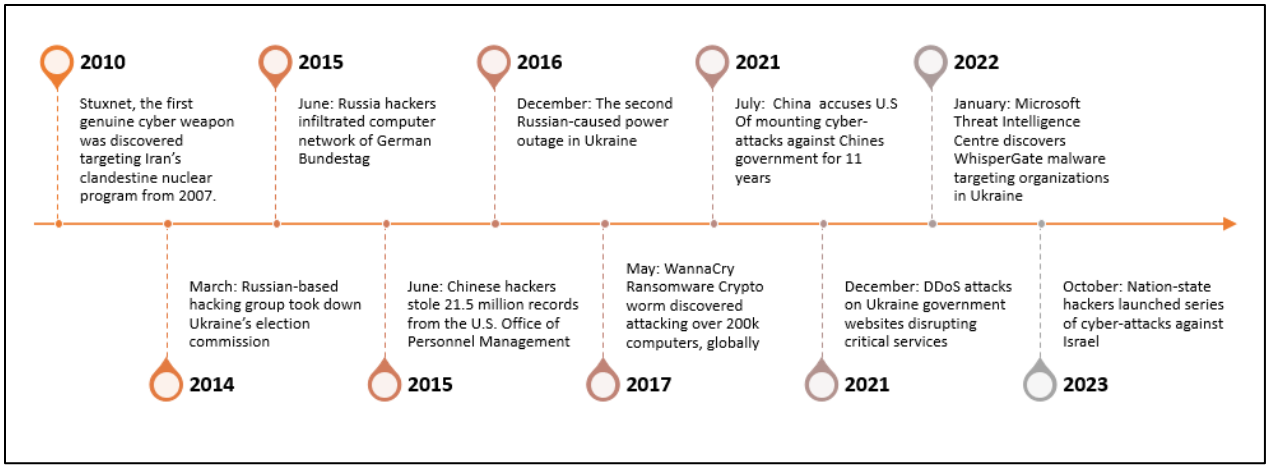


Figure 3: Timeline of Cyber Weapons (Adapted)[18]

Over the past decade (2010s to 2020s), major military powers have increasingly integrated cyber capabilities into their military strategy. Cyber operations are now considered a key component of hybrid warfare, complementing traditional kinetic actions. Military doctrines have been updated to include guidelines for cyber operations, and there is a growing emphasis on joint and combined arms operations, including cyber elements[19]. Nevertheless, African militaries lag in the development of cyber warfare capabilities. This is also demonstrated in the National Cyber Power Index (NCPI)[20], where only one African country is found in this index.

**Digital Transformation in the African Battlespace**

With digital transformation as the emerging approach to improving military capabilities, the cyber threat landscape continues to evolve[21],[22],[23],[24]. Many militaries are struggling with issues related to escalation and deterrence in the cyber domain[21]. The attribution of cyber-attacks, the development

[18] Huseyin Kuru, 'Evolution of war and cyber-attacks in the concept of conventional warfare,' *Journal of Learning and Teaching in Digital Age*, 3(1), (2018): pp. 12-20.
[19] James Black, et al., 'Multi-Domain Integration in Defence: Conceptual Approaches and Lessons from Russia, China, Iran and North Korea', RAND Corporation, 2022, https://www.rand.org/pubs/research_reports/RRA528-1.html, accessed 17 January 2024.
[20] Julia Voo, Irfan Hemani and Daniel Cassidy, 'National Cyber Power Index 2022', Cambridge: Belfer Center for Science and International Affairs, Harvard Kennedy School, https://www.belfercenter.org/publication/national-cyber-power-index-2022, accessed 17 January 2024.
[21] NIST, 'Computer Security Resource Centre (CSRC)', Gaithersburg: National Institute of Standards and Technology, (2023).
[22] Thaba Mphahlela and Jabu Mtsweni, 'Developing Robust Cyber Warfare Capabilities for the African Battlespace,' *22nd European Conference on Cyber Warfare and Security (ECCWS 2023)*, June 2023.
[23] Interpol. 'African Cyberthreat Assessment Report: interpol's key insight into cybercrime in Africa', (Singapore: Interpol, 2021).
[24] CrowdStrike, '2023 Global threat report', https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrike2023GlobalThreatReport.pdf, accessed 28 November 2023.

of norms and rules of engagement, and the establishment of deterrence strategies are ongoing challenges in the field of cyberwarfare[25]. The evolution of military operations to include cyberwarfare reflects the increasing interconnectedness of the modern world and the recognition that conflicts extend beyond traditional domains. As technology continues to advance, the integration of cyber capabilities into military operations is likely to become even more pronounced[26].

The 21st Century has experienced more infiltration of advanced technologies in the African battlespace resulting from militaries driving transformation of their capabilities. Cyber warfare capability development in Africa is necessitated by the speed of digital transformation in the content. Over the past decade, Africa has observed digitalisation at highest scales and influenced by increasing connectivity that offers both opportunities and challenges for military operations. This is also influenced by awareness and recognition of cybersecurity and potential impact of cyber threats on national security; capacity building to address the challenge of skills shortages in the cyber workforce; regional and international cooperation on cyber norms, legislation development, standards, skills transfer and capability development to govern cyberspace and protect critical infrastructure.

The section that follows discusses the cyber warfare capabilities in perspective focusing on three pillars. This perspective is provided since cyber warfare capabilities are new for many African militaries, but even for developed countries, what constitute cyber warfare capability is still not fully understood including how a nation goes about the establishment, deployment, and sustainment of such capabilities for national interests.

**Cyber Warfare Capability Perspective**

Within the cyberspace, a plethora of capabilities could be observed from a security-perspective, and the most common capability is that of cybersecurity that deals with solutions that minimises danger or threat to organisational assets from threat actors. This capability is a necessity across all economic sectors as well as in the military.

---

[25] Chris Jaikaran, 'Cybersecurity: Deterrence Policy', (Washington, United States: Congressional Research Service), 18 January 2022, https://crsreports.congress.gov/product/pdf/R/R47011, accessed 17 January 2024.

[26] Grace B Mueller, Benjamin Jensen, Bandon Valeriano, Ryan C. Maness, and Jose Macias, *Cyber operations during Russo-Ukrainian war: from strange patterns to alternative futures,* (Washington, United States, Center for Strategic & International Studies, 2017).

***Cyberwarfare capability framework***

The framework for cyberwarfare capability[27], and the military's role in the cyberspace, follows the same analogy for war in other domains. The framework to be considered must cover the full spectrum of the ability of the military to conduct operations in and through the cyberspace.

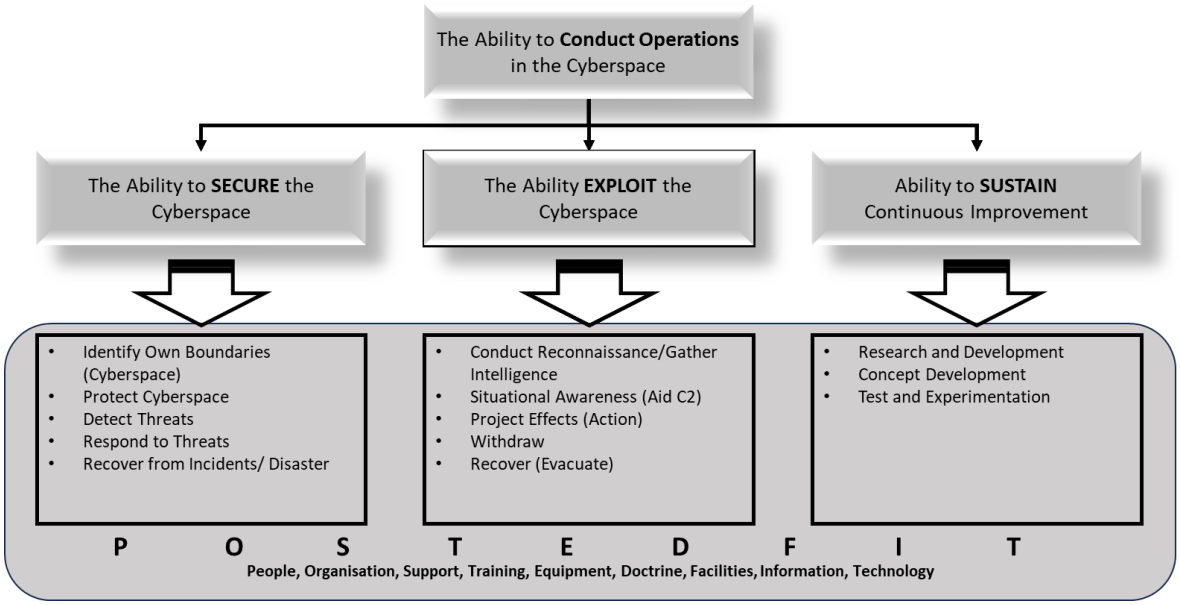


Figure 4: Cyber Warfare Capabilities Framework[27]

The framework, depicted in Figure 4 above is summarised in terms of three areas supported by the POSTEDFIT elements: (1) **Secure cyberspace**: the main goals in cyberspace should firstly focus on defending territorial integrity and sovereignty of a nation and playing and effective role in the domain. These goals are no different to militaries in defending their nations in the air, sea, land, and/or space. (2) **Exploit cyberspace:** any nation-state that needs to exert its power in cyberspace must have the capabilities of offensive weaponry. The first element of this capability is reconnaissance and threat intelligence. African militaries need to understand the enemy through continuous scouting of intelligence and areas of interest. This intelligence would allow for situational awareness across all domains of war and enable the forces to focus on the crown jewels of the enemy in the cyberspace. The exploitation of the enemy needs to be executed both in peace and war time, but in a covert manner. (3) **Sustain and maintain cyber warfare capability**:

[27] Thaba Mphahlela and Jabu Mtsweni, 'Developing Robust Cyber Warfare Capabilities for the African Battlespace,' *22nd European Conference on Cyber Warfare and Security (ECCWS 2023)*, June 2023.

African militaries need to ensure that there are continuous improvements in their cyber warfare capabilities, through research development, and innovation (RD&I), concept development and experimentation in building, executing, and sustaining the cyber warfare capability. Training of cyber warriors and investment in local cybersecurity industry is critical in sustaining a local cyber warfare capability.

According to Oosthuizen & Roodt[28], any capability may be conceived of as comprising nine POSTEDFIT constituent elements. As such, establishing cyber warfare capabilities requires a comprehensive approach, that integrates al elements of a capability. These elements are People (P), Organisation (O), Support (S), Training (T), Equipment (E), Doctrine (D), Facilities (F), Information (I), Technology (T). In integrating these elements, a cyber warfare capability that is resilient, proactive, and able to adapt to the evolving nature of cyber threats can be established.

- *People:* Identify and recruit skilled individuals with expertise in cyber warfare, including ethical hackers, threat analysts, and incident responders.
- *Organisation*: Determine a suitable organisation appropriately structured to deal with the complexities of the cyberspace. The organisation must foster collaboration between different teams, such as IT, security, legal, and intelligence, to ensure a comprehensive approach to cyber warfare.
- *Support:* The complexity of cyber operations requires support to be designed as an integral part of the cyberwarfare capability. This must be done by establishing ongoing training programs to keep personnel updated on the latest threats[29], technologies, and defensive strategies.
- *Training:* The rapid rate at which the cyberspace evolves due to the fast-changing technology landscape, requires fit for purpose, future oriented training and training tools and infrastructure capable of preparing capabilities for effective cyber operations[30].

[28] Rene Oosthuizen and Jan HS Roodt, 'Credible Defence Capability: Command and Control at the Core'*, Brisbane, Land Warfare Conference*, (2008).
[29] Julian Jang-Jaccard and Surya Nepal, 'A survey of emerging threats in cybersecurity', *Journal of Computer and System Sciences,* (2014): pp. 973-93.
[30] Erica Lonergan and Jacquelyn Schneider, 'The Power of Beliefs in US Cyber Strategy: The Evolving Role of Deterrence, Norms, and Escalation', *Journal of Cybersecurity,* 9(1), (2023).

- *Equipment (Hardware)*: As cyber warfare is a rapidly evolving phenomenon, the hardware or equipment used to play in the cyberspace must be adaptable to emerging threats and technologies. The integration of hardware with skilled personnel and effective processes is crucial for a robust cyber warfare capability[31].

- *Doctrine (Processes):* In the military, doctrine is important to guide how missions and operations are executed. As such, as African armed forces develop cyber capabilities, it is essential that they focus on the development of processes and procedures for robust cyber warfare capabilities. The foundation of cyber warfare doctrine is informed by a national strategy on cyber warfare. In addition, doctrine development and improvement need to consider staying abreast of relevant cybersecurity regulations, international laws, and compliance standards[32].

- *Facilities*: In establishing the cyber warfare capability, facilities should be designed with a focus on physical and cybersecurity to safeguard sensitive information and operations. The identification, protection, and monitoring of critical information infrastructure, which are source of nation-state cyber-attacks, is another critical element that African militaries need to have their hands-on.

- *Information*: Effective cyber warfare capabilities rely on continuous intelligence gathering, analysis, and updating to stay ahead of evolving threats. It is crucial to ensure that information is accurate, timely, and relevant to the specific objectives of the cyber warfare campaign. Additionally, ethical, and legal considerations should guide the collection and use of information during cyber warfare operations[31].

- *Technology*: The technologies required for cyber warfare capabilities should include offensive and defensive tools, communication systems, encryption technologies, and advanced analytics[33]. The integration of technology with skilled personnel, comprehensive

---

[31] The White House Washington, 'National Cybersecurity Strategy', https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf, accessed 28 November 2023

[32] Jabu Mtsweni, Noxy Gcaza and Mphahlela Thaba, 'A unified cybersecurity framework for complex environments'. *In Proceedings of the Annual Conference of the South African Institute of Computer Scientists and Information Technologists*, (2018).

[33] Florian Egloff and James Shires, 'Offensive Cyber Capabilities and State Violence: Three Logics of Integration',. *Journal of Global Security Studies,* 7(1) (March 2022), https://doi.org/10.1093/jogss/ogab028 .

processes, and ongoing training is critical for building and maintaining a robust cyber warfare capability[34].

Over and above these requirements, the availability of resources such as a budget, leadership, and political direction for the military is critical to establish a cyber warfare capability. Cyber warfare strategy is the cornerstone of the above, as without it, cyber warfare capability cannot be established in a strategic manner.

***National cyber power index***

In the recent research study conducted by Voo, Hemani, and Cassidy[35], the NCPI highlights the increasing emphasis of nation-states on developing cyber warfare capabilities in the context of contemporary conflicts. The NCPI serves as a metric to gauge a nation's demonstrated and potential proficiency in various aspects of cyber operations, encompassing strategies, defensive and offensive measures, resource allocation, private sector capabilities, workforce, and innovation.

The NCPI serves as a comprehensive tool for assessing and understanding the evolving landscape of cyber capabilities on a global scale. The varied dimensions of cyber operations underscore the multifaceted nature of national efforts in building and demonstrating cyber power in contemporary geopolitical contexts. **Error! Reference source not found.** shows the scatter plot of cyber power rankings of 30 countries, and it is evident that African nation states are non-existent, except for Egypt, who is shown as having a lower capability and lower intent in cyber power, whilst countries such as the United States (US), United Kingdom (UK), Russia, and China are well advanced having higher capability and higher intent to use cyber means to demonstrate power in the cyberspace. These countries have a direct interest in cyber warfare capabilities for Africa as observed by their support and/or attacks in the African cyber space.

[34] Jabu Mtsweni and Mphahlela Thaba, 'Building an Integrated Cyber Defence Capability for African Missions,' *Journal of Information Warfare* 21(1) (2021): pp. 17-34.

[35] Julia Voo, Irfan Hemani and Daniel Cassidy, 'National Cyber Power Index 2022', Cambridge: Belfer Center for Science and International Affairs, Harvard Kennedy School, https://www.belfercenter.org/publication/national-cyber-power-index-2022, accessed 17 January 2024.

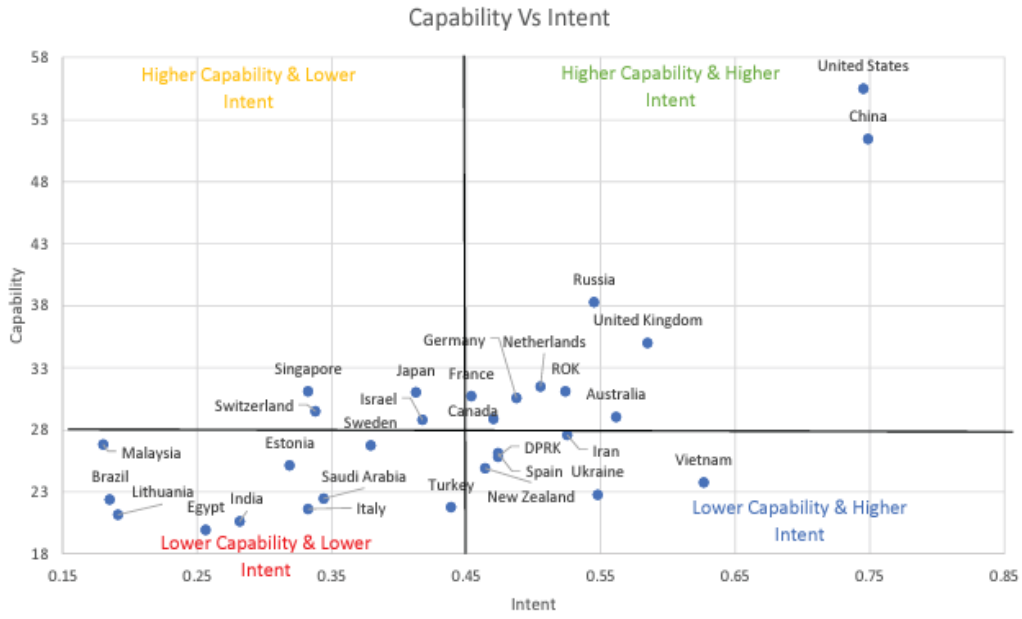


Figure 5 Nations Cyber Warfare Capability vs Intent[36]

## Cyber Warfare Challenges in Africa

The African cyberspace faces increasing cyber threats[37], and several cyber incidents have been observed at government levels including attacks on militaries and sovereignty of African countries through election attacks, critical information infrastructure attacks, and cyber-terrorism[38],[39],[40]. The loss of huge financial resources in Africa due to cyber-crime is also widely reported in the academic and business space. As a results of these cyber-attacks, African countries have made notable progress in developing legal measures such as policies and laws to deal with cybersecurity incidents including data protection. Nevertheless, our research indicates that with regards to cyber

[36] Julia Voo, Irfan Hemani and Daniel Cassidy, 'National Cyber Power Index 2022', Cambridge: Belfer Center for Science and International Affairs, Harvard Kennedy School, https://www.belfercenter.org/publication/national-cyber-power-index-2022, accessed 17 January 2024.
[37] Interpol. 'African Cyberthreat Assessment Report: interpol's key insight into cybercrime in Africa', (Singapore: Interpol, 2021).
[38] Club of Mozambique, 'Mozambique: Hackers demand ransom – AIM report,' https://clubofmozambique.com/news/mozambique-hackers-demand-ransom-aim-report-210221/, accessed 18 March 2023.
[39] Bassant Hassib and James Shires, 'Manipulating uncertainty: cybersecurity politics in Egypt', *Journal of Cybersecurity*,7(1), (2021): pp. 1-16, https://doi.org/10.1093/cybsec/tyaa026 .
[40] Kaluka Wanjala, 'Kenya Airports Authority suffers data breach from notorious hacking group', 13 April 2023, https://www.techarena.co.ke/2023/04/13/kenya-airports-authority-suffers-data-breach-from-notorious-hacking-group/, accessed 14 July 2023.

warfare, only a handful African countries have publicly known cyber warfare efforts, and other cybersecurity instruments to secure the cyberspace are still taking long to approve and implement[41].

The use of cyber means by foreign state-actors, non-state actors and extremists' groups for malicious attacks against African states is more apparent. For example, a Yemen Cyber Army claimed responsibilities for cyber-attacks on several websites from various government entities and ministry of defence in Mozambique[42]. In Nigeria, it was reported that Boko Haram hacked the personnel records database of Nigeria's secret service[43] and this has subsequently led to the Nigerian Chief of the Army ordering the creation of the Cyber Warfare Command as well as the Cyber Warfare School[44]. In 2020, Samme-Nlar reported that both state actors and non-state actors are increasingly targeting African states using cyber weapons[45]. An example of the attack on the Ethiopian Cyberinfrastructure by the Egyptian non-state actors over a grand renaissance dam dispute was provided. In this case study, it is also made clear that African states are unprepared to deal with cyber-attacks.

The dearth of cyber skills workforce in African militaries for securing and exploiting the cyberspace is a well-researched topic. And this is compounded by the high global and regional cybersecurity skills shortages[46],[47]. Most of the skills required are in the architecture engineering, management, and security operations, which are critical within the military domain[48]. Moreover, Africa militaries' path to developing robust cyber warfare capabilities is hindered by a range of

---

[41] Heloise Pieterse, 'The cyber threat landscape in South Africa: A 10-year review', *The African Journal of Information and Communication,* (2021): pp. 1-21.
[42] Club of Mozambique, 'Mozambique: Hackers demand ransom – AIM report,' https://clubofmozambique.com/news/mozambique-hackers-demand-ransom-aim-report-210221/, accessed 18 March 2023.
[43] Denise Baken, 'Cyber Warfare and Nigeria's Vulnerability', *E-International Relations,* (3 Nov 2013), https://www.e-ir.info/2013/11/03/cyber-warfare-and-nigerias-vulnerability/, accessed 18 January 2024.
[44] Nigerian Army, 'The transformation of Nigeria Army Cyber Warfare Command under Major General Ayannuga.' https://army.mil.ng/?p=5757, accessed 18 March 2023
[45] Tomsli Samme-Nlar, 'The future of armed conflict in Africa: what cyber-attacks on Ethiopian government tell us', 08-10-2020, https://aanoip.org/the-future-of-armed-conflict-in-africa-what-cyber-attacks-on-ethiopian-government-tell-us/, accessed 18 March 2023.
[46] Michael de Jager, Lynn Futcher, and Kerry-Lynn Thomson, 'An Investigation into the Cybersecurity Skills Gap in South Africa'. In: S. Furnell & N. Clark, eds. *Human Aspects of Information Security and Assurance. HAISA 2023. IFIP Advances in Information and Communication Technology,* (Springer, Cham, 2023).
[47] Raphael Kaibiru et al. 'Closing the Cybersecurity Skill Gap in Kenya: Curriculum Interventions in Higher Education', *Journal of Information Security,* 14(2), (April 2023): pp. 136-151.
[48] Christopher A Ramezan, 'Examining the Cyber Skills Gap: An Analysis of Cybersecurity Positions by Sub-Field', *Journal of Information Systems Education,* 34(1), (Winter 2023): pp. 94-105.

infrastructure challenges, including limited access to ICT infrastructure and home-grown cyber tools. The Global Cybersecurity Index (GCI)[49] revealed that out of 54 African states, only 19 have Computer Security Incident Response Teams (CSIRTs) or Computer Emergency Response Teams (CERTs) to enable them to respond to incidents at the national level. Based on GCI, only 10 African countries are addressing critical infrastructure resiliency in their national cybersecurity strategies. The challenges in African cyber battlespace are further compounded by inadequate budgets and funding, weak laws and regulations, and a lack of regional cooperation on cybersecurity.

**Case Studies on Cyber Warfare in Africa Battlespace**

In the cyberspace, militaries need to contend with a diverse range of adversaries, not just nation-states. These adversaries may include hackers, terrorists, businesses, social groups, criminals, and even unsuspecting computer users. The inability to clearly define the enemy is the reason some nations may respond to the consequences of cyber-attacks rather than addressing the root causes. As Sun Tzu astutely observed in The Art of War, "*If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle."*[50].

Therefore, it is crucial that when African militaries are developing cyber warfare capabilities, they do not solely focus on nation-states as adversaries but also consider other potential threat actors, including nation-state-sponsored cyber hacktivist groups, insider threat, and understand their threat landscape including the critical infrastructure. This section delves into a multi-case study examining four African countries to explore and comprehend how their militaries have adapted to tackle the challenges posed by cyberspace for national security.

***Selection of countries***

To effectively analyse the maturity of cyber warfare capabilities in Africa, a strategic selection of countries is crucial. Considering factors such as the GCI[49] the Global Firepower Index (GFPI)[51]

[49] ITU, 'Global Cybersecurity Index 2020'. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf, accessed 24 November 2023.
[50] Sun Tzu, *The Art of War* (Hachette: Obooko, 1994).
[51] Global Firepower, '2023 Military Strength Ranking', https://www.globalfirepower.com/countries-listing.php, accessed 18 January 2024.

and the recent research work of the International Institute of Strategic Studies[52], four countries stood out for in-depth study: Egypt, South Africa, Nigeria, Kenya, and Egypt. Egypt, with a GCI score of 95.48 and a GFPI ranking of 14, exemplifies the role of international collaborations in enhancing cyber warfare capabilities. Its strategic partnerships with regional and global powers provide valuable insights into collaborative cyber security measures. South Africa, with a a GCI score of 78.46 and a Global fire power ranking of 33, is a regional leader in cybersecurity and military power. It has established a dedicated cyber command unit and makes it an ideal candidate for examining cyber warfare preparedness.

Nigeria, ranking number 36 in the GFPI and has a score of 84.76 by GCI, represents a rapidly developing cyber power in Africa. Its growing economy and increasing internet penetration make it susceptible to cyberattacks, necessitating a thorough understanding of its cyber warfare strategy and threat landscape. Kenya is ranked number four in the African continent by ITU on the GCI released in 2020. However, it has been declining in the GFPI, ranking number 87 in 2023. Kenya was therefore selected as it highlights the challenges faced by many African nations in developing robust cyber defences. By examining these four countries through the lens of the POSTEDFIT capability elements including cyber warfare strategy, threat landscape, collaborations, and other relevant factors, a comprehensive understanding of cyber warfare capability in Africa can be achieved.

***Case study approach***

In conducting the case studies, we opted to use the cyber warfare capability framework proposed by Thaba and Mtsweni[53]. The framework is depicted in Figure 4 and adopts a 3-level ranking system for the POSTEDFIT capability elements and associated functions. These elements are classified as 0) no functions implemented 1) Limited functions 2) Intermediate functions and 3) full functions.

[52] The International Institute for Strategic Studies, 'Cyber Capabilities and National Power Volume 2', 7 September 2023, https://www.iiss.org/research-paper/2023/09/cyber-capabilities-national-power-volume-2/, accessed 18 January 2024, Singapore.

[53] Thaba Mphahlela and Jabu Mtsweni, 'Developing Robust Cyber Warfare Capabilities for the African Battlespace,' *22nd European Conference on Cyber Warfare and Security (ECCWS 2023)*, June 2023.

Table *1*: Cyber warfare capability maturity framework

| | POSTEDFIT Elements | | Overall Capability Maturity | Range | Scale |
|---|---|---|---|---|---|
| | | | MLI 0 | 0%-20% | Very Weak |
| 3 | Full | | MLI 1 | 21%-40% | Weak |
| 2 | Intermediate | | MLI 2 | 41%-60% | Moderate |
| 1 | Limited | | MLI 3 | 61%-80% | Strong |
| 0 | None | | MLI 4 | 81%-100% | Very Strong |

This case study applies the framework to assess the "AS-IS" cyber warfare capability of the selected countries using publicly available data. The framework is used to evaluate a country's cybersecurity and cyber warfare capabilities by rating capability-related functions as shown in Table 1 and aggregating them to determine the maturity level of each sub-capability. It also incorporates the National Institute of Standards and Technology (NIST) cybersecurity maturity model's 5-level ranking system[54].

The proposed framework uses a "four-force model" scale to narratively describe the different maturity level indicators (MLI). The assessment using the proposed framework is complemented by an assessment of the country's cyber threat landscape, examination of each country's cyber warfare and cybersecurity strategies as well as regional and international partnerships.

***Case study results***

This section presents the findings of the case study encompassing four countries, analysed through the POSTEDFIT model. The assessment focuses on the selected countries' ability to secure and defend their cyberspace, exploit cyberspace opportunities, and maintain and enhance their cyber defense capabilities. The quantitative results based on the proposed framework as discussed above are presented in Table 2 below supported by the qualitative narrative based on publicly available information. The results a combination of the three pillars: secure cyberspace, exploit cyberspace, and sustain/maintain cyber warfare capability.

[54]'NIST Cybersecurity Framework,' https://www.nist.gov/cyberframework, accessed 01 June 2023.

Table *2*: Case Study Quantitative Results

| Country | Capability | Capability Elements | | | | | | | | | Additional Elements | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Secure/Exploit/Sustain Cyber Defence Capability | People | Organisation | Support | Training | Equipment | Doctrine (Policies and Procedures) | Facilities | Information | Technologies | Regional and International Collaborations | Strategy |
| South Africa | 48 | 5 | 5 | 5 | 5 | 5 | 4 | 5 | 5 | 3 | 4 | 2 |
| Kenya | 45 | 4 | 4 | 4 | 5 | 4 | 5 | 4 | 5 | 3 | 5 | 2 |
| Nigeria | 44 | 4 | 4 | 5 | 5 | 3 | 4 | 5 | 5 | 3 | 4 | 2 |
| Egypt | 64 | 6 | 6 | 7 | 7 | 5 | 7 | 7 | 6 | 5 | 6 | 2 |

***Egypt***

Based on our case analysis, we identified that Egypt has one of the leading cyber warfare capabilities in Africa with a score of 64 based on the POSTEDFIT assessment. Our analysis is that Egypt has good support from government in securing and exploiting the cyberspace. Training of cyber warriors is intentional and advancing. There are efforts in the development of local technologies, albeit still limited. The cyber structures seem coordinated and functional, and Egypt has aligned itself with cyber power nations such as UK and US and seem to counter cyber-activities forcefully demonstration their cyber intelligence capabilities. The cyber threat landscape in Egypt is touted as being amongst the 20 most vulnerable countries to cyber-attacks[55]. As a case in point, in 2020, Trend Micro detected and blocked over 20 million cybersecurity threats in the Egyptian cyberspace[56] and this had increased to 56 million cybersecurity threats in 2022[57], representing a 180% increase in 2 years. The main cyber threats in Egypt are sabotage to cyber infrastructure, cyber terrorism, cyberwar, and digital identity theft. Based on recent research reports, Telecon Egypt suffered a data breach that impacted millions of users. This indicates that the cyber threat landscape in Egypt is concerning.

Egypt has therefore acknowledged and expressed that the security of the cyberspace is critical to national security and the national economic system. As such the country has passed a series of cyber laws and a cyber security strategy developed by the Egyptian Supreme Cybersecurity Council (ESCC)[58] to deal with aspects such as monitoring of social networks, messaging

[55] Daily News Egypt, 'Egypt among 20 most vulnerable countries to cyber-attacks: NTRA', 27 September 2022, https://www.dailynewsegypt.com/2022/09/27/egypt-among-20-most-vulnerable-countries-to-cyber-attacks-ntra/, accessed 01 December 2023.
[56] Trend Micro, 'Trend Micro blocks 22 million threats in Egypt during 2020', https://egyptian-gazette.com/technology/trend-micro-blocks-22-million-threats-in-egypt-during-2020/, accessed 01 December 2023.
[57] Trend Micro, 'Trend Micro blocks over 56 million threats in Egypt, Reveals Annual Cybersecurity Report', https://www.trendmicro.com/en_ae/about/newsroom/press-releases/2023/05-06.html, accessed 1 December 2023.
[58] Egyptian Supreme Cybersecurity Council, 'National Cybersecurity Strategy 2017-2021', (Cairo: Arab Republic of Egypt, 2023), https://mcit.gov.eg/Upcont/Documents/Publications_12122018000_EN_National_Cybersecurity_Strategy_2017_2021.pdf, accessed 18 January 2024.

applications, and web-threats[59] in the digital transformation era. These laws are also to some extent influenced by Arab Spring in Egypt and Tunisa between 2010 and 2013[60]. In addition, the country has a cybersecurity strategy being implemented in line with their vision 2030 on digital transformation for the entire country. The Egyptian government has the Computer Emergency Readiness Team (EG-CERT) established in 2009, and the institution started with 6 persons and had at least 100 cyber warriors in 2021. The EG-CERT has a mandate of training government agencies on cybersecurity issues. EG-CERT has worked collaboratively with other state agencies to conduct cybersecurity drills, which are necessary for building cyber workforces and prepare for incident response[61]. In addition, Egypt claims to have experts trained to extract digital evidence from all kinds of electronic devices.

Egypt leadership have acknowledged the shores of cyber skills and are establishing two cybersecurity centres of excellence to address the issue[62]. Egypt has demonstrated the zeal to build cyber warfare capabilities and are cooperating locally with universities in the field of cybersecurity and with several large countries, such as the United States of America as part of the EG-CERT. The cyber warfare capabilities in Egypt have been in development over the past few years, and this is also demonstrated in the NCPI. Egypt appears in the top six of countries with a strong cyber surveillance capability behind largest nations such as China and the US. This capability has been strengthened and demonstrated in Egypt since the Arab Spring revolution with the countering of cyber-activism blocking social media platforms during the protests[63]. Moreover, Egypt has established a competitive cyber defence capability behind Australia, Ukraine, US, France, UK, and Netherlands based on the NCPI due to its strong partnership with the US, UK, and Israel.

Scientific research and development as well as cybersecurity industry development is part of the Egyptian cybersecurity strategy, and already indicated Egypt have plans in place to establish other

---

[59] Adele Forveille, 'Egypt's cyberpower ambitions', 15 May 2023, https://incyber.org/en/egypt-cyberpower-ambitions/, accessed 1 December 2023.
[60] Sahar Khamis, 'Revisiting Cyberactivism Six Years after the Arab Spring: Potentials, Limitations and Future Prospects,' In: N. Lenze, C. Schriwer & Z. Jalil, eds. Media in the Middle East: Activism, Politics, and Culture. (Palgrave, Macmillan, 2017), https://doi.org/10.1007/978-3-319-65771-4_1 .
[61] Rasha Mahmoud, 'Egypt ramps up cyber, data security capabilities', AL-Monitor, 12 April 2022, https://www.al-monitor.com/originals/2022/03/egypt-ramps-cyber-data-security-capabilities, 01 December 202.
[62] Daily News Egypt, 'Egypt among 20 most vulnerable countries to cyber-attacks: NTRA', 27 September 2022, https://www.dailynewsegypt.com/2022/09/27/egypt-among-20-most-vulnerable-countries-to-cyber-attacks-ntra/, accessed 01 December 2023.
[63] Bassant Hassib and James Shires, 'Manipulating uncertainty: cybersecurity politics in Egypt', *Journal of Cybersecurity*,7(1), (2021): pp. 1-16, https://doi.org/10.1093/cybsec/tyaa026 .

centres of excellence in cybersecurity. These are commendable initiatives for continuous development and maintenance of existing cyber capabilities. In terms of home-grown cyber defence technologies, Egypt has a defence company in ACME SAICO that recently launched a system for command, control, communications, computer, cyber, intelligence, and reconnaissance (C5ISR)[64]. However, experts suggest that Egypt still relies heavily on foreign-based technologies[65]. The main weaknesses in the maturity of cyber warfare capability in Egypt includes lack of cybersecurity awareness, especially by government officials who have been detected using unprotected e-mails and servers, and cyber-attacks on critical information infrastructure.

***South Africa***

Our case analysis indicates that South Africa's cyber warfare capability is *moderate* with a score of 48 based on the POSTEDFIT elements. In terms of securing the cyberspace, several efforts have been made, but there is still silos and misalignment within government agencies in addressing cyber threats. Relevant structures have been established such as a national CSIRT that is also certified by the Forum of Incident Response and Security Teams (FIRST)[66], a global forum for cyber incident response and security teams, but its effectiveness and impact is still not felt by industry and citizens. The State Security Cybersecurity Centre is also operational and regularly shares vulnerability disclosures, but the capabilities appear limited, particularly when it comes to national cyber incident response. South Africa has also done well in participating in several cyber initiatives including those by ITU as evidence in the GCI, however development of the cybersecurity strategy has taken too long to be finalised. The government of South Africa developed and approved the NCPF in 2015 to respond to such cyber threats and guide the country's cybersecurity strategy development, nevertheless, framework lapsed without being fully implemented.

---

[64] D Liam, 'Egypt unveils hybrid C5ISR system at IDEX 2023', 27 February 2023, https://www.military.africa/2023/02/egypt-unveils-hybrid-c5isr-system-at-idex-2023/, Accessed 1 December 2023.

[65] Florentia Neagu and Anca Savu, 'The costs of cyberterrorism for the national economy: United States of America vs Egypt,' *In Proceedings of the International Conference on Business Excellence*, (29 November 2019): pp. 983-993.

[66] 'FIRST is the global Forum of Incident Response and Security Teams,' https://www.first.org/, accessed 18 January 2024.

In relation to the threat landscape, research reports indicate that South Africa, Nigeria, and Kenya are the most targeted countries in the cyberspace[67]. The Cyber Exposure Index released in 2020 indicates that South Africa is the sixth most exposed country in the cyberspace. Nevertheless, the index features a limited number of countries[68]. In South Africa, researchers further report that cyber-attacks against state and private organisations have increased by over 95% between 2010-2020 with attacks ranging from website hacks, denial of service attacks, data breaches, and ransomware attacks[69]. Through the NCPF, South African government has established a Cybersecurity Hub coordinated by the Department of Communications and Digital Technologies to handle cyber issues concerning citizens and private sector[70] and is operational to a limited extent. In addition, a Cybercrimes Act of 2020 was signed into law by the President of South Africa in 2021 for dealing with increasing cybercrimes, and currently it is being implemented with the establishment of the Designated Point of Contact for cybercrimes reporting, investigation, and monitoring as well as international and regional cooperation[71].

The Cyber Command within the South African National Defence Force (SANDF) is also being established to coordinate the country's military cyber defense efforts. The Cyber Command is responsible for protecting critical military infrastructure, developing cyber warfare tactics and techniques, and training military personnel in cybersecurity[72]. In South Africa, the last Defence Review was done in 2014, and when it comes to cyber warfare, the review suggested that South Africa requires the protection of its cyber-domain, through a comprehensive information warfare capability, integrated into its intelligence-related information systems at the international, national and defence levels[73]. By 2023, it was apparent based on media reports and parliamentary feedback

---

[67] Africa News, 'Kenya hit by record 860m cyber-attacks in a year', 03 October 2023, https://www.africanews.com/2023/10/03/kenya-hit-by-record-860m-cyber-attacks-in-a-year/, accessed 18 January 2024.
[68] Cyber Intelligence House, 'Cyber Exposure Index,' https://cyberexposureindex.com/, accessed 01 December 2023.
[69] Heloise Pieterse, 'The cyber threat landscape in South Africa: A 10-year review', *The African Journal of Information and Communication,* (2021): pp. 1-21.
[70] South African Government, 'National Cybersecurity Policy Framework', 04 December 2015, https://www.gov.za/documents/national-cybersecurity-policy-framework-4-dec-2015-0000, accessed 18 January 2024.
[71] South African Government, ' Cybercrimes Act 19 of 2020', 01 June 2021, https://www.gov.za/sites/default/files/gcis_document/202106/44651gon324.pdf, accessed 18 January 2024.
[72] S Lesedi, 'Funding mars SANDF Cyber Command', 13 January 2023, https://www.military.africa/2023/01/funding-mars-sandf-cyber-command/, accessed 01 December 2023.
[73] South African Government, 'South African Defence Review 2014', 25 March 2014, https://www.gov.za/documents/other/south-african-defence-review-2014-25-mar-2014, accessed 18 January 2023.

that the Department of Defence (DoD) Cyber Command still faces several challenges, such as lack of resources, funding, and skills[74].

South Africa cyber warfare coordination efforts are limited, particularly because the cyber warfare strategy is still not finalised by 2023. The research and developments efforts, even though visible and conducted by organisations such as the Council for Scientific and Industrial Research (CSIR), are still not impactful in the cyberspace due to the limited coordination between government, academia, and the private sector. The lack of cyber warriors or force in the Cyber Command is also apparent with training conducted across different domains, but not much operationalisation.

***Kenya***

Our quantitative analysis of Kenya suggests that they have a *moderate* leaning towards weak cyber power with a score of 45 using the POSTEDFIT maturity assessment. Kenya was found to be limited to intermediate on peoples training, organisational structures, and good on having strategies in place and doctrines on the cybersecurity side. Cyber warfare capabilities are still limited, but international collaborations are beginning to be consistent especially their partnership with the United States, one of the stronger cyber powers, according to all measures[75]. Africa News reported that Kenya was being hit by over 860 million attacks in 2023 disrupting over 5,000 online government services[76]. This makes Kenya to be the third most vulnerable country in Africa after South Africa and Nigeria. In Kenya, government digital services and critical information infrastructure were disrupted by suspected nation-state actors known as Anonymous Sudan 30-days after their launch, resulting in a direct impact on citizens[77],[78].

---

[74] S Lesedi, 'Funding mars SANDF Cyber Command', 13 January 2023, https://www.military.africa/2023/01/funding-mars-sandf-cyber-command/, accessed 01 December 2023.
[75] The International Institute for Strategic Studies, 'Cyber Capabilities and National Power Volume 2', 7 September 2023, https://www.iiss.org/research-paper/2023/09/cyber-capabilities-national-power-volume-2/, accessed 18 January 2024, Singapore.
[76] Africa News, 'Kenya hit by record 860m cyber-attacks in a year', 03 October 2023, https://www.africanews.com/2023/10/03/kenya-hit-by-record-860m-cyber-attacks-in-a-year/, accessed 18 January 2024.
[77] Kaluka Wanjala, 'Kenya Airports Authority suffers data breach from notorious hacking group', 13 April 2023, https://www.techarena.co.ke/2023/04/13/kenya-airports-authority-suffers-data-breach-from-notorious-hacking-group/, accessed 14 July 2023.
[78] Kenya News, 'Cyber Attack: 8 Major Cyber Attacks That Have Occurred in Kenya in Recent Years', 28 July 2023, https://www.ghanamma.com/ke/2023/07/28/cyber-attack-8-major-cyber-attacks-that-have-occurred-in-kenya-in-recent-years/ accessed 08 August 2023.

In attempting to address the concerning cyber threat landscape, a national cybersecurity strategy that outlines the country's approach to protecting its cyberspace, and a KDF strategic vision was developed and some of its elements implemented. This has led to the establishment of a National Computer and Cybercrimes Coordination Committee (NC4) as per the Computer Misuse and Cybercrimes Act of 2018 to coordinate the government's response to cyber threats[79]. This structure is a multi-agency entity to deal address effective detection, prohibition, prevention, response, investigation and prosecution of computer misuse and cybercrimes, including facilitating international cooperations. Some notable entities part of the structure are the National Intelligence Service and Kenya Defence Forces (KDF).

In addition, Kenya has established the national Computer Incident Response Team-Coordination Centre (KE-CIRT/CC) as a crucial point for reporting and responding to cyber incidents[80]. This structure is certified by FIRST and part of ITU, US Cybersecurity Infrastructure and Agency (CISA) as well as East African Communications Organisation. A National Defence University is already engaged in building cybersecurity capabilities collaborating with different stakeholders, albeit these are still at preliminary stages[81]. Although Kenya has embraced digital transformation in various aspects of the battlespace, cyber warfare capability development still is limited and as KDF modernises the critical information infrastructure and adopt IT business processes, the development of cyber capabilities becomes paramount to secure the Kenyan cyberspace. In relation to international partnerships, Kenya has cemented an effective cooperation with the US having held two sessions in 2023 on cyber and digital dialogues, digital capacity development, responsible state behavior in the cyber space, collaboration on combating cybercrime and others[82]. Despite the progress that has been made, Kenya still faces several challenges in protecting its cyberspace, including lack of skilled cybersecurity professionals and outdated ICT infrastructure.

---

[79] 'National Computer and Cybercrimes Coordination Committee, https://nc4.go.ke/about/, accessed 01 December 2023.
[80] Communications Authority of Kenya, 'The National KE-CIRT/CC,' https://ke-cirt.go.ke/, accessed 01 December 2023.
[81] Kenya Defence Force, 'Strategic Vision', Chief of the Defence Forces, June 2021, https://www.mod.go.ke/wp-content/uploads/2021/06/CDF-Strategic-Vision.pdf, accessed 01 December 2023.
[82] Office of the Spokesperson, 'The United States Joins Kenya for Third Cyber and Digital Dialogue in Nairobi', https://www.state.gov/the-united-states-joins-kenya-for-second-cyber-and-digital-dialogue-in-nairobi/, accessed 01 December 2023.

***Nigeria***

Our analysis based on the robust cyber warfare capability development framework; Nigeria is assessed to be at a moderate level a few elements behind Kenya with a combined rating of 44 on POSTEDFIT elements assessment. The strengths of Nigeria in the cyber warfare domain are the training of cyber warriors and development of cyber surveillance capabilities and have been intentional about the cyber-defence capability development in their national strategy. The weaknesses are ineffective international relations, lack of stronger cyber warfare partnerships, and operational cyber structures. With regards to the threat landscape, Nigeria has experienced numerous incidents of cyber-terrorism, mostly instituted by the militants' group such as Boko Haram[83]. At the same time, Nigeria is recording an increase in digitally facilitated crimes and high cyber-attacks due lack of cyber surveillance in the Nigeria's cyberspace[84]. The Independent National Electoral Commission (INEC) website was hacked during a presidential election and the government claimed this was done by Boko Haram[85]. During the same elections in 2023, Nigeria government announced that it experienced over 12 million cyber-attacks[86].

In responding to the cyber threats and attacks, Nigeria has developed a national cybersecurity strategy that is aligned to the international norms and frameworks, covering elements of cyber-crime, protection of critical infrastructure, development of national and international partnerships, capacity development, R&D, and conducting cybersecurity exercises[87]. This strategy was updated in 2021 to consider enhancing cyber-defence capabilities[88].

The Office of the National Security Adviser (ONSA) in Nigeria is responsible for cybersecurity. In addition, Nigeria has setup the Nigerian Computer Emergency Response Team (ngCERT), but

---

[83] Kate O'Flaherty, 'The Nigerian Cyber Warfare Command: Waging War In Cyberspace', Forbes, 26 November 2018, https://www.forbes.com/sites/kateoflahertyuk/2018/11/26/the-nigerian-cyber-warfare-command-waging-war-in-cyberspace/?sh=55b693a22fba, accessed 01 December 2023.

[84] Aamo Iorliam, 'Cybersecurity in Nigeria: A Case Study of Surveillance and Prevention of Digital Crime,' *Springer Briefs in Cybersecurity,* (Springer, 2019).

[85] Kate O'Flaherty, 'The Nigerian Cyber Warfare Command: Waging War In Cyberspace', Forbes, 26 November 2018, https://www.forbes.com/sites/kateoflahertyuk/2018/11/26/the-nigerian-cyber-warfare-command-waging-war-in-cyberspace/?sh=55b693a22fba, accessed 01 December 2023.

[86] Jimisayo Opanuga, 'Nigeria records 12.9 million cyberattacks during presidential election', The Guardian, 14 March 2023, https://guardian.ng/news/nigeria-records-12-9-million-cyberattacks-during-presidential-election/, accessed 02 December 2023.

[87] Oluwafemi Osho and Agada Onoja, 'National cyber security policy and strategy of Nigeria: a qualitative analysis,' *International Journal of Cyber Criminology* 9(1), (2015): pp. 120-143.

[88] The International Institute for Strategic Studies, 'Cyber Capabilities and National Power Volume 2', 7 September 2023, https://www.iiss.org/research-paper/2023/09/cyber-capabilities-national-power-volume-2/, accessed 18 January 2024, Singapore.

it is argued that it has not been that effective and other structures such as the National Cybersecurity Coordination Centre had not been setup by late 2023[89]. The Nigerian Army established Nigerian Army Cyber Warfare Command (NACWC) in 2018 with the mandate to tackle terrorism, banditry, and other attacks by criminal actors. This came at a time when propaganda and fake news trailed the fight against insurgency and other political happenings. The command unit was tasked to protect data space and prevent cyber terrorism[90]. However, reports indicate that in Nigeria there is no Defence CSIRT, which is critical for cyber-incident response within the military.

Reports suggest that it has over 150 trained cyber warriors in the Nigerian Army with the responsibility to "monitor, defend, and assault in the cyberspace"[91], but criticism has been that these personnel do not have prior knowledge or experience in cybersecurity issues, let alone cyber warfare[92]. With regards to cyber technology acquisition, Nigeria seems to have focused mostly on cyber intelligence capability to counter terrorism. Furthermore, Nigeria has an appetite for international collaborations in the cyberspace with the US, Israel, and UK to name a few, but these cooperations seem not to have been fully exploited other than on training to improve the cyber warfare capabilities in Nigeria. Moreover, Nigeria faces challenges in the cyber battlespace such as foreign-dominant cyber tools, and its military cyber warfare strategy remains limited. This is purely because national structures for dealing with cyber warfare are not fully consolidated, limited skilled cyber warriors and over-reliance on foreign-based technologies for the cyberspace[93].

---

[89] Jimisayo Opanuga, 'Nigeria records 12.9 million cyberattacks during presidential election', The Guardian, 14 March 2023, https://guardian.ng/news/nigeria-records-12-9-million-cyberattacks-during-presidential-election/, accessed 02 December 2023.

[90] Nigerian Army, 'The transformation of Nigeria Army Cyber Warfare Command under Major General Ayannuga.' https://army.mil.ng/?p=5757, accessed 18 March 2023

[91] Kate O'Flaherty, 'The Nigerian Cyber Warfare Command: Waging War In Cyberspace', Forbes, 26 November 2018, https://www.forbes.com/sites/kateoflahertyuk/2018/11/26/the-nigerian-cyber-warfare-command-waging-war-in-cyberspace/?sh=55b693a22fba, accessed 01 December 2023.

[92] Office of the Spokesperson, 'The United States Joins Kenya for Third Cyber and Digital Dialogue in Nairobi', https://www.state.gov/the-united-states-joins-kenya-for-second-cyber-and-digital-dialogue-in-nairobi/, accessed 01 December 2023.

[93] The International Institute for Strategic Studies, 'Cyber Capabilities and National Power Volume 2', 7 September 2023, https://www.iiss.org/research-paper/2023/09/cyber-capabilities-national-power-volume-2/, accessed 18 January 2024, Singapore.

**Discussion and Implications**

The cyberspace will continue to increase in dominance as domain of war. As such African military forces and governments must prepare now to operate in the cyberspace in this digital transformation era. If not, they will be left behind and suffer the consequence of unable to deal with the complex threat landscape that not only impact on national security, but territorial integrity, national sovereignty, and economic development. To develop maturing cyber warfare capabilities, *visionary leadership* is paramount, and in Africa, only Egypt has that visionary leadership where cyber warfare development with is led with intent from the top grounded in an actionable national strategy[94]. In Nigeria, cybersecurity initiatives are coordinated within the Office of the National Security Advisor, which is a promising idea, however, criticism has been that this is infested with personnel that do not have much experience in the domain, and as such this can be a hinderance towards a mature cyber warfare capability.

The critical success factor for African militaries in building offensive and defensive cyber capabilities is *full support and investment* by the government. In our analysis, we noted that many of the initiatives in Africa on cyber warfare are not effective because there is lack of full support and funding by the national government, at the same time, cyber capabilities are not elevated to be part of the top priorities. Adequate funding is paramount to develop skills, but also relevant infrastructure staffed with cyber warriors and to build the local cyber industry, which is critical in sustaining the cyber defence capability. For African militaries to increase their dominance in the African cyberspace as well as globally, *proper coordination between different national security structures* within a country as well as regionally is important. Except for Egypt, our observations are that most African countries do not have proper coordination on cyber defence issues. This is a limitation than an advantage in the domain where shortage of skills is a global issue[95]. Operations in and through the cyberspace requires collaboration between militaries and civilian organisations, including private organisations. The integrating character of the cyber domain, means operations in all the other domains, land, sea, air, and space, must always integrate cyber warfare capabilities, and without effective coordination it will be difficult to sustain and maintain this capability.

---

[94] Adele Forveille, 'Egypt's cyberpower ambitions', 15 May 2023, https://incyber.org/en/egypt-cyberpower-ambitions/, accessed 1 December 2023.

[95] Raphael Kaibiru et al. 'Closing the Cybersecurity Skill Gap in Kenya: Curriculum Interventions in Higher Education', *Journal of Information Security,* 14(2), (April 2023): pp. 136-151.

Research, development, and innovation on cyber warfare is critical for African nations, especially as our findings indicate that most of the African militaries are reliant on foreign technologies. In addition, a bibliometric analysis[96] by authors of this chapter indicates that Africa has limited RD&I on cyber warfare. To sustain and maintain cyber warfare capabilities strategic R&DI in this domain cannot be overly emphasised. Cyber warfare capabilities must be acknowledged as emerging specialised combat capabilities, that must be integrated at all levels of war. The boundaryless nature of the cyberspace, make it even more critical for all domain capabilities to be supported by cyber warfare capabilities. The level of employment of cyber warfare capabilities must be dependent on the mission to be undertaken, and the level of objectives to be achieved. Therefore, cyber warfare capabilities must be employed autonomously or in support of operations by African forces. This concept may require a study on its own, to unpack and the implications to be considered.

This is due to the capabilities required, the expertise for development of appropriate tools, deployment of these tools, infrastructure required to plan, conduct, and support cyber operations, and other capabilities that may be required that are owned and operated by private industry. African countries require substantial improvements in digital infrastructure, large-scale investment in cyber-security talent and development of a domestic cyber-technology market to play a meaning role and protect the continent and its citizens.

## Conclusion

The chapter emphasised the imperative for African militaries and governments to continuously invest in cyber warfare capabilities to remain competitive in the global cyberspace. This necessitates addressing existing resource, expertise, and infrastructure gaps, fostering a culture of cybersecurity, and developing comprehensive cyber strategies aligned with national security objectives. By effectively leveraging cyber warfare capabilities, African armed forces can safeguard their security, enhance operational effectiveness, and contribute to regional stability. African countries have responded to these challenges at distinct levels, albeit still limited. National security agencies in Africa have focused on improving cybersecurity awareness and training, implementing basic defensive measures, and acquiring limited cyber capabilities Some African

[96] Jabu Mtsweni and Mphahlela Thaba, 'Bibliometric Analysis of Cyber Warfare Research in Africa: Landscape and Trends,' *International Conference on Cyber Warfare*, (2024).

countries have also established cyber warfare units, developed cyber strategies, and enhanced inter-agency cooperation. Mostly importantly, African governments have integrated cyber considerations into national security policies and doctrines, but a lot of work is still required to get to the required levels exhibited by cyber super-powers such as the US, China, and Russia.

**Bibliography**


Caplan, N., 2013. Cyber War: The Challenge to National Security. Global Security Studies, pp. 93-115.

Egloff, F. J. & Shires, J., 2022. Offensive Cyber Capabilities and State Violence: Three Logics of Integration. Journal of Global Security Studies, 7(1).

Hassib, B. & Shires, J., 2021. Manipulating uncertainty: cybersecurity politics in Egypt. Journal of Cybersecurity, 00(0), pp. 1-16.

Kuru, H., 2018. Evolution of war and cyber-attacks in the concept of conventional warfare. Journal of Learning and Teaching in Digital Age, 3(1), pp. 12-20.

Lonergan, E. D. & Schneider, J., 2023. The Power of Beliefs in US Cyber Strategy: The Evolving Role of Deterrence, Norms, and Escalation. Journal of Cybersecurity, 9(1).

Mbanaso, U. M., 2016. Cyber warfare: African research must address emerging reality. South African Journal of Information and Communication, Issue 18.