Developing Robust Cyber Warfare Capabilities for the African Battlespace

Mphahlela Thaba[1] and Jabu Mtsweni[1,2]
[1] Council of Scientific and Industrial Research, Pretoria, South Africa
[2] Security Institute for Governance and Leadership in Africa (SIGLA), Faculty of Military Science, Stellenbosch University

jthaba@csir.co.za
mtswenij@gmail.com

Abstract: The evolution of technology in the African battlespace continues to pose a significant challenge to the African militaries. This evolution increases the need for the African militaries to be able to operate in the cyberspace strategically and effectively. Developing cyber warfare capabilities remains a challenge to many African militaries who are struggling to remain afloat due to ever decreasing resources, including budgets. This in turn reduces the effect of these militaries in the evolving battlespace. This paper seeks to present a comprehensive framework for developing cyber warfare capabilities for African militaries to be able to operate efficiently in the cyber battlespace. The proposed POSTEDFIT aligned framework, requires a comprehensive system thinking approach towards developing capabilities in a phased manner. This includes the ability to define the capabilities in terms of the requirements presented by the cyberspace, and the components forming these capabilities. The generic framework is based on the basic understanding of a capability, as the ability to do something, in this case, the ability to secure and operate in the cyberspace for African militaries, ability to conduct offensive cyber operations and ability to keep abreast with the evolving cyber battlespace.

Keywords: Cyber Security, Cyber Warfare, Cyber Operations, Cyber Defence, Cyber Attacks, Africa Battlespace

1. Introduction

The interest in cyber warfare is demonstrated in various ways, and we are seeing other countries collaborating with their allies in developing cyber warfare capabilities. According to Ndebele (2023), the US Army has pledged to support selected African countries to improve their defences against extremists and terrorism in the cyber space, maritime, and land. Some of the countries targeted by this initiative include Botswana, Rwanda, Kenya, and others.

Nevertheless, there are still gaps in cyber warfare capabilities for most African countries. In fact, African countries are lagging far behind that only one African country appears in the top 30 of countries with the higher National Cyber Power Index (i.e., Egypt) (Voo, Hemani, & Cassidy, 2022). In addition, the African countries do not have established doctrines on cyber operations, lack of skills and capacity are a serious impediment, and reliance on foreign technologies is still a pain point for most African countries.

This paper therefore seeks to present a comprehensive framework for developing cyber warfare capabilities to enable African militaries to operate in the cyberspace, either to secure and/or to exploit for advancing military interests.

The rest of this paper is structured as follows: Section 2 provides context and overview on the definitions of terms used in this paper. In Section **Error! Reference source not found.**, the importance of cyber warfare in modern conflicts is narrated including the status quo in the African context. Section 4 highlights the research methodology adopted for this study in conducting the literature review as well as in conceptualising the proposed generic cyber warfare capability development framework. In Section 5, the different approaches that are used in cyber operations are demonstrated and discussed. Section 6, the proposed comprehensive, yet generic, framework is presented and supported with the POSTEDFIT capability elements. The paper is concluded with future research recommendations in Section 7.

2. Definitions and context

The arena of the cyberspace is quite diverse with different interpretations, capabilities, and skills requirements. The understanding of this operational environments has an influence on how African nations could build capabilities for securing their tailored militaries.

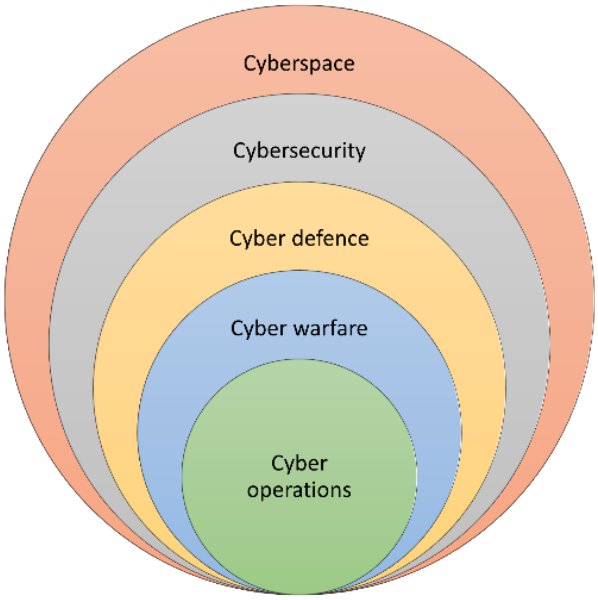

Figure 1: Cyber Warfare Context (source: authors)

In essence as depicted in Figure 1, cyberspace is a domain of operation and is simply defined as a *"notional environment that enables people and systems to communicate over interconnected networks"*, according to a Dictionary of Psychology (Colman, 2014). In the military context, it is classified as the fifth operational domain of warfare (Hall, 2016) and interacts with other domains of warfare such as space, air, land, and sea.

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 minimizes danger or threat to organizational assets from threat actors. This capability is a necessity across all economic sectors as well as in the military. In terms of this paper, two positions are considered when it comes to offensive cyber, and that is cyber defence and cyber warfare**.** In this research, we perceive the cyber defence capability to be adopting in the main a defensive posture within the cyber battlespace as relied upon by the North Atlantic Treaty Organization (NATO, 2022).

On the contrary, cyber warfare, which is the focus on this paper, is define as a capability of a nation-state to exploit another nation-state's communication networks, computer systems and/or other critical information infrastructure for purposes of causing delay, disruption, and/or damage (Wang, 2023). According to (Oosthuizen & Roodt, 2008), capability may be conceived of as comprising nine POSTEDFIT (Personnel, Organisation, Sustainment, Training, Equipment, Doctrine (Policies), Facilities, Information and Technology) constituent elements. Lastly, cyber operations are critical in every phase of the modern warfare and are in this paper 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 (Shankar, 2023).

The understanding of cyber warfare is therefore related to the understanding of the environment within which this war takes place, the cyberspace. The United States of America (USA) Department of Defence (DOD) through its Joint Chiefs of Staff, in the Joint Publication 3-12, for cyber operations, highlights that cyberspace, while part of the information environment, is dependent on the physical domains of air, land, maritime, and space. This publication further indicates that the cyber operations use links and nodes located in the physical domains and perform logical functions to create effects first in cyberspace and then, as needed, in the physical domains (US DOD, 2018).

3. Importance of cyber warfare capabilities in modern conflicts

The ongoing Russia-Ukrainian conflict and growing geo-political tensions places a new emphasis on critical industries and national security, leading to more strict security requirements and restrictions. According to Burt (2022), an increase in military-coordinated cyber-attacks, and a continued growth of conflict in cyberspace has been observed over the recent past. In the Russia-Ukraine conflict that escalated in early 2022, we have observed that this conflict is hybrid using physical weapons as well as cyber-attacks. For instance, in January 2022, it is reported that a cyber-attack targeted the Ukrainian government, hitting 90 websites and deploying

malicious software masquerading as ransomware to damage dozens of computers in government agencies. Moreover, in February 2022, a DDoS attack knocked down websites belonging to the Ukrainian Defence Ministry and two of the country's largest banks offline. In China and US, we have seen threat actors spreading mobile malware to citizens using fake cell phone towers, as well as sending hate-SMS-messages from rogue base stations (Chirgwin, 2017; Koebler, 2015).

As per the recent research study by Voo, Hemani and Cassidy (2022), the National Cyber Power Index (NCPI) demonstrates that nation-states are serious about building cyber warfare capabilities for the modern conflicts. The NCPI measures nations demonstrated and potential capability in strategies, defensive and destructive operations, resource allocation, private sector capabilities within a country, workforce, and innovation. Possible cyber operations that a nation would be having to demonstrate cyber power include surveillance and monitoring of domestic groups, strengthening and enhancing national cyber defences, controlling and manipulating the information environment, foreign intelligence collection for national security, growing national cyber and commercial technology competence, destroying or disabling an adversary infrastructure and capabilities, defining international cyber norms and technical standards, and amassing through cyber operations.

Figure 2 below 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 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.

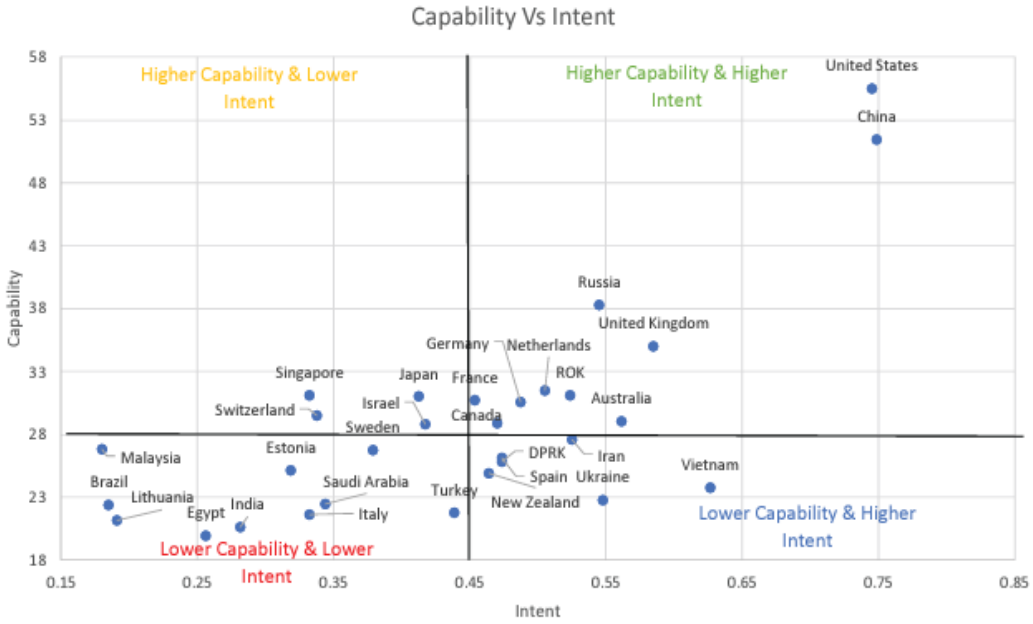

Figure 2: Nations Cyber Warfare Capability vs Intent (Voo et al, 2022)

3.1 Overview of existing cyber warfare capabilities in Africa

In Africa, we have started to observe the establishment of cyber warfare capabilities and use of cyber operations by extremists' groups and nation-states. For example, a Yemen Cyber Army claimed responsibilities for cyber-attacks on several websites from various government entities and ministry of defence in Mozambique in Mozambique (AllAfrica, 2022).

In Nigeria, it is reported that Boko Haram hacked the personnel records database of Nigeria's secret service (Baken, 2013) and this has subsequently led to the Nigerian Chief of the Army (Nigerian Army, 2022) ordering the creation of the Cyber Warfare Command as well as the Cyber Warfare School.

In 2020, Samme-Nlar (2020) reported that both state actors and non-state actors are increasingly targeting African states using cyber weapons. 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.

In South Africa, the last Defence Review was done in 2014 (South African Government, 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. In line with the Defence Review, the National Policy Cybersecurity Policy Framework (NCPF) was published in 2015 (State Security Agency, 2015), and it defined DOD's overall responsibility as the coordination, accountability, and implementation of cyber defence measures in South Africa such as the establishment of the Cyber Command. By 2022, it was apparent based on media reports and parliamentary feedback that the cyber command still faces several challenges, such as lack of resources and skills (DefenceWeb, 2023).

In South Africa, researchers further report that cyber-attacks against state and private organizations have increased by over 95% between 2010-2020 with attacks ranging from website hacks, denial of service attacks, data breaches, ransomware attacks (Pieterse, 2021). Researchers also report that South African public platforms such as websites have seen an increased targeted cyber-attacks mainly because over 80% of public websites are vulnerable (Mtsweni, 2015). As such, governments across the globe continue to invest in cyber warfare capabilities. Over 60 countries, a number that is rising, currently have some mechanism to play in the digital warfare and intelligence gatherings. Nevertheless, African countries always lag in this regard.

4. Research Methodology

The research presented in this paper follows the Design Science Research (Hevner et al., 2010) which subscribes to the concept of an artefact. In this paper, the comprehensive framework for developing cyber warfare capabilities is considered as an artefact. The artefacts are derived through reference to the literature, existing frameworks, as well our experience in the cyber security and military environment within the African continent.

Design science research methodology was chosen for this research work because it is a "*problem-solving approach that seeks to enhance human knowledge via creation of innovative artefacts*" (vom Brocke; Hevner; Maedche, 2020). The key steps that were followed for the purposes of this research study will focus on people, processes, and technology.

These key steps will be enhanced by a POSTEDFIT approach that is commonly used in building military capabilities (Willers et al, 2011; Mtsweni et al, 2018). In the design phase of the DSR, a cyber warfare capability development framework is proposed and evaluated through use case scenario analysis as per the guidelines found in (Hevner et al., 2010).

It is important to note that not all POSTEDFIT elements are the same under different contexts. It is therefore critical to look at them closely under each environment, and they may also not be weighted the same by different nation states depending on their intentions and missions in the cyber space. It is worth noting that in this paper, leadership and budget elements are in the people and support elements respectively.

4.1 Systems thinking approach.

Systems thinking approach (Litster, Hurst, & Cardoso, 2023) is applied in this research to understand and develop a comprehensive framework for developing cyber warfare capabilities, which are complex in nature. The dynamic nature of the cyber threats, and the evolving cyberspace continues to challenge the traditional ways of determining solutions and thus a systems thinking approach has been chosen a guideline to evolve the comprehensive cyber warfare capability framework.

This approach suggests that we need to understand the functionality required from the strategic direction provided by the organisation before we think about the solutions required. The ability of any military and/nation, to conduct operations in the cyberspace must be guided by that nation's national security strategy. From this understanding, it also follows that the cyber warfare capabilities are derived from the functionality implied in the missions defined to achieve the set national strategic objective (Smit et al, 2012). Figure 3 shows an example of the decomposition of the national objectives to capabilities. Military capabilities are then decomposed further into system of systems, then systems, right down to components. This approach is therefore demonstrated in the proposed framework.

Figure 3: Systems thinking for cyber warfare capability development (Smit et al, 2012).

5. Cyber Warfare Capability Mapping

In this section, we highlight and briefly discuss the different approaches that are used in cyber operations, and we map these against different cyber warfare capability objectives and functions.

Cyber warfare capabilities may differ from one nation state to the other as observed in the National Cyber Power Index (Voo et al, 2022) depending on the capability levels and intentions. The overall NCPI assessment measures the 'comprehensiveness' of a country as a cyber actor. Comprehensiveness, in the context of NCPI, refers to a country's use of cyber to achieve multiple objectives as opposed to a few. The most comprehensive cyber power is the country that has (1) the intent to pursue multiple national objectives using cyber means and (2) the capabilities to achieve those objective(s) (Voo et al, 2022).

In addition, the cyber domain has seen a myriad of “kill chains” that demonstrate different tactics that could make a nation-state successful or not when they are conducting cyber operations.

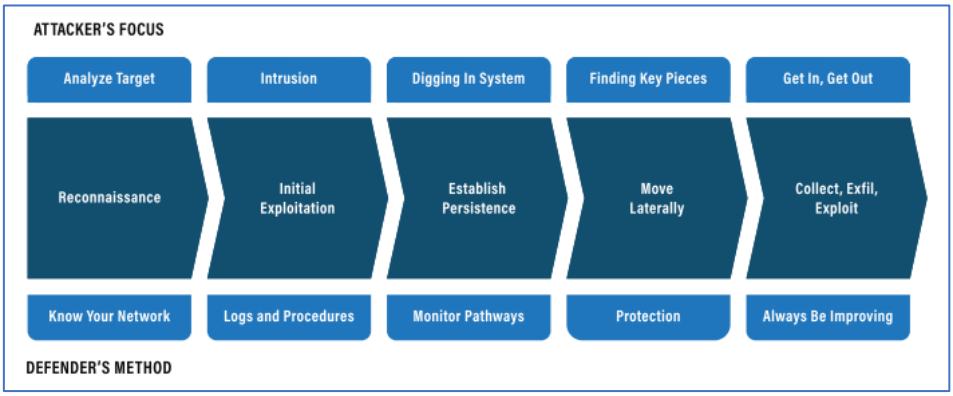

Figure 4: The Intrusion Model (Tarnowski, 2017)

As depicted in Figure 4, it is also observed that cyber operations share similar characteristics with conflicts in the physical domains but differs in others. For instance, information and communication technologies have dual use where they may be exploited to aid common business operations but could also be exploited to advance strategic military missions. Whilst in the physical realm, miliary equipment (e.g., fighter aircraft) has a strategic military purpose in mind. In the cyber domain, the universe of adversaries is also quite wide, unlike in the physical domain where location, proximity or historical conflicts may provide signs of who is likely to attack you or not. The essence in the intrusion model is that it is two sides of the same coin, and this means that nation states need to have both the defensive and offensive posture. As an attacker, the military, in the cyberspace, needs to be able to analyse the target through intelligence gathering, but at the same time the same nation needs to fully understand its assets (e.g., networks or critical information infrastructure) including their whereabouts and status at all time or failure to know this can result into devastating defeat in the cyberspace.

In the cyber space, militaries need to deal with myriad of adversaries and not only nation state actors. These may include hackers, terrorists, businesses, social groups, criminals, and even unsuspecting computer users. The inability to define the enemy is the reason some of the nations may deal with the consequences of cyber-attacks rather that then root causes. As narrated by Sun Tzu 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." Thus, it is critical that when African militaries are building cyber warfare capabilities, they do not only focus on only the nation-states as an adversary, but other threat actors as well that could be nation-state sponsored such as cyber hacktivists groups.

Lastly, in the cyberspace, nations' assets may be infiltrated in peace time and used in war time, thus the situational awareness in the cyberspace needs to be wider than just an internal view. This also means it is becoming more difficult to have a complete view on who may attack a nation or already attacked a nation in the cyberspace. It is also complex to attribute responsibility of cyber-attacks, as in the cyberspace attackers can even use various techniques including proxies to divert attention. Moreover, the motives for cyber operations can be quite wide including economic, military, national secrets and political advantage, and the cyberspace allows for cyber operations to be ensued based on any of these motives, because in the cyberspace, offensive operations are significantly easier than defence, mainly because anyone can advance them, whilst in the traditional warfare, defence is the default position, and a successful attack requires supremacy in people, technology, doctrine, or strategy.

6. Comprehensive framework for developing cyber warfare capabilities for African Militaries

6.1 Cyber warfare capability framework requirements for operationalization

The framework for cyberwarfare capability, 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 the cyberspace. These operations must address both the offensive and defensive capabilities.

The ability by the military to conduct operations in the cyberspace, requires the following (this understanding is on the premise that higher political and strategic intent is understood including the military in the cyberspace):

- The understanding of the political, and strategic objectives of the country.
- The understanding of the cyberspace, what constitutes the domain.
- The legal framework, governing roles of various entities.
- The ability to secure its own systems.
- The ability to conduct reconnaissance and gather intelligence against adversaries.
- The ability to do target acquisition.
- The ability to launch offensive actions against target adversaries.
- The ability to defend offensive actions of the adversary or its associates.
- Recovery from an onslaught or cyber-attacks.
- Withdrawal from cyber operations when the situation dictates.
- Continuous improvement of the capability.

Over and above these requirements, the availability of resources such as a budget for the military is critical to establish a cyber warfare capability. In has been noted, for instance, in South Africa that Defence Intelligence has struggled to setup a fully functional Cyber Command due to lack of budget allocated for such a capability (DefenceWeb, 2023).

6.2 Design of the framework

In designing the comprehensive framework for developing cyber warfare capabilities for the African militaries, several considerations were made, including existing capabilities based on publicly available information, capability objectives in the cyberspace, ranking of African militaries in relation to the National Cyber Power Index, and national and international norms and standards.

In formulating this framework, the authors followed a three-layered approach that focused *on 1) national strategic goal in the cyberspace, 2) cyber warfare capability objectives for a nation-state, and 3) minimum cyber warfare capability functions* that nation-state need to possess to demonstrate a cyber warfare capability in the battlespace. Additionally, the capability functions were mapped against the POSTEDFIT capability elements as depicted in Figure 5.

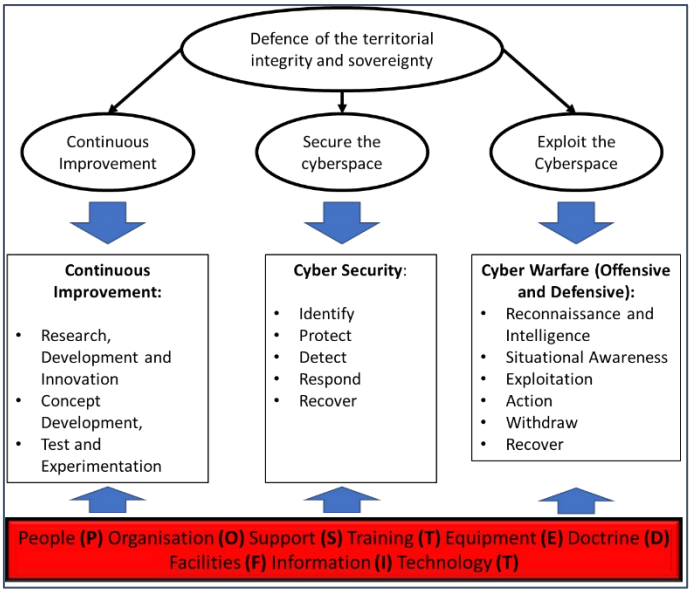

Figure 5: Proposed comprehensive cyber warfare capability framework.

In brief, the model suggests that for African militaries to establish, deploy and sustain their cyber warfare capabilities, the main goals in the cyberspace should be about defending territorial integrity and sovereignty. These goals are no different to militaries in defending their nations in the air, sea, land, and/or space. In particular, the core objectives for playing an effective role in the cyberspace, African militaries need to ensure that there are continuous improvements, through RD&I, concept development and experimentation in building, executing, and sustaining the cyber warfare capability. This capability is seen in two lenses: *(1) securing the cyber space (i.e., taking a security and protection approach)*, and *(2) exploiting the cyberspace to gain territorial and sovereignty advantage through offensive means*.

Any nation-state that needs to exert its power in the cyberspace must have the capabilities as depicted in the cyber kill chain or intrusion model (see Figure 4). The preliminary function 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. Countries such as China, Russia and United States are super-powers in the cyberspace, and they also take advantage of the capable privately accessible offensive capability to exploit their adversaries in peace times and easily destroy the target in war times. And as such, African militaries need to also strategic form partnership with local and international industries to enhance and continuously improve the cyber warfare capability.

6.3 Understanding the cyber warfare capability development framework

To implement the framework, we draw up a capability matrix that is mapped to capability attributes (functions) and capability elements. These elements are weighted, because we are of the view that they are not of equal importance in the cyber domain, and in certain instances their importance is given effect by the cyber mission. In this research paper, we recommend that any capability should have a higher value or proportion on people, technology, and processes. Using the POSTEDFIT framework, this perspective would map to people, doctrine, and technology.

6.4 Framework use case scenario analysis

To demonstrate the utility of the framework, we choose *Country X in Africa* that is still establishing its cyber warfare capability and evaluated it using the proposed framework. It should be noted that we demonstrate the framework by using officially known capabilities and in instances where no information is available assumptions using lessons from cyber-attacks that we have observed online.

Table 1: Framework maturity level index for POSTEDFIT elements and overall capability

	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

In demonstrating the framework, the first step is measuring the cyber warfare capability using the capability attributes scales chosen for each of the elements under each capability as depicted in Figure 5. The framework adopts a 3-level ranking system for the POSTEDFIT capability elements and associated functions, and these are classified as *0) No functions implemented 1) Limited functions 2) Intermediate functions and 3) full functions* (see **Table 1:** *left*). This means that to assess if a country has cyber security or cyber warfare capability, one will rate the capability associated functions between 0-3. These are then aggregated to determine the maturity level of each sub-capability. In addition, the framework uses the 5-level ranking system as found in the NIST cybersecurity maturity model (Almuhammadi, 2017), classified as maturity level indicator (MLI) (MLI0-MLI4) *(*see Table 1: *right*).

In the proposed framework, the authors opted to use a "four force model[1]" scales to narratively indicate the meaning of the different MLI levels, and these are very weak for none to minimal capability to very strong for advance or full capability. For example, within a range of 0-20, this means that the maturity level of the cyber warfare capability for Country X is *Very Weak*, whilst 61-80 will be considered as S*trong*. As already indicated, these ranges could be adjusted to suit the dynamics of different African states. It also needs to be borne in mind that this framework could be used to measure the "AS-IS" cyber warfare capability or alternatively the "TO-BE" capability of a country of interest.

Table 2: Implications and implementation of the framework

				Capability Elements									
				People	Organisation	Support	Training	Equipment	Doctrine (Policies and Procedures)	Facilities	Information	Technologies	Maturity
Capability Maturity Level Indicator	Goals	Capability	Capability Attributes	15%	10%	10%	15%	5%	15%	5%	10%	15%	100%
	Security	**Ability to secure the cyber space**											45%
		30%	Identify	2	2	2	2	2	2	2	2	2	
			Protect	2	1	1	2	1	2	2	2	2	
			Detect	1	1	1	2	1	1	1	2	2	
			Respond	1	1	1	1	0	1	0	2	1	
			Recover	1	0	0	1	0	1	0	2	0	
	Exploitation	**Ability to conduct Offensive and Defensive Cyber Operations**											34%
39%		50%	Reconaissance and Intelligence	2	2	2	2	1	2	2	2	2	
			Situational Awareness	1	0	1	1	1	2	1	2	1	
			Exploitation	1	0	1	1	1	0	0	2	1	
			Cause of Effects	1	1	1	1	1	1	0	2	1	
			Sustain and Defend	1	1	0	1	0	1	0	1	1	
			Withdrawal	1	0	0	0	0	0	0	1	1	
	Continuous Improvement	**Ability to keep abreast with the evolving cyber battlespace**											39%
			Research, Development and Innovation	2	1	1	2	2	1	2	2	2	
		20%	Concept Development	2	1	1	0	1	0	1	2	1	
			Test and Experimentation	1	1	1	1	1	0	1	2	1	

The application of the model as demonstrated in Table 2 above is progressive, and accumulates from the scores for the capability elements, adding up to overall cyber warfare. As indicated in the Table 2, the total scores for the POSTEDFIT elements per capability, are weighted and thereafter added to give a total score for the individual capability attributes. For example, in Table 2, it can be observed that Country X scores *Moderate* (45%) on the

[1] https://revisionscience.com/a2-level-level-revision/physics-level-revision/particles-radiation-quantum-phenomena/four-force-model

sub-capability to secure the cyber space, but is measured to be *Weak* (34%) on the ability to conduct offensive cyber operations as well as in their ability to keep abreast with evolving cyber battlespace.

After the individual sub-capabilities are scored, their scores are weighted against the determined proportion of contribution of each capability to the overall capability. In this paper, the weighting for sub-capability one is 30%, sub-capability 2 is 50%, and sub-capability 3 is 20%. The outcome is the overall capability maturity level indicator, which in this example in Table 2 is 39%. This score indicates the overall level of a nations' ability to defend the territorial integrity, and sovereignty of the country within cyberspace. In this instance, *Country X* is measured to be *Weak* on the overall capability, and this implies that they may not be able to effectively operate offensively and/or defensively in the cyber battlespace.

7. Conclusion and Future Research

The evolution of the operational environment, and the emergence of the cyberspace as a domain of war, remains critical to the strategic direction of many militaries. The African battlespace is not immune to this development, and the global nature of the cyberspace forces all African militaries to include cyberwarfare capabilities in their portfolio. This paper provided a framework, to define these capabilities, in terms of the capability attributes, and the capability elements, and provides a link between the capabilities and the national strategic objectives. The framework is also instrumental in measuring the level of maturity of the capability, and determines capability gaps, which will help nations draw up development plans to address the gaps. The framework is at this stage still simplistic, in terms of the calculations and the definitions of various measures used in the calculations. This implies that the validation of the model will still be done as part of the continuous research on the model. Further to the proposed framework, more research must still be undertaken to understand the cyber warfare capabilities, and related attributes, to enable for measuring effectiveness and/or efficiency of the capabilities.

References

Ajijola, A.H and Allen, N.D.F. 2022. African Lessons in Cyber Strategy. African Centre for Strategic Studies. Available online: https://africacenter.org/spotlight/african-lessons-in-cyber-strategy/

AllAfrica. 2022. Mozambique: Hackers Demand Ransom. Available online: https://allafrica.com/stories/202202230552.html

Almuhammadi, S. and Alsaleh, M., 2017. Information security maturity model for NIST cyber security framework. *Computer Science & Information Technology (CS & IT)*, *7*(3), pp.51-62.

Baken, D.N. 2013. Cyber warfare and Nigeria's vulnerability. E-International Relations. ISSN 2053-8686

Burt, T.2023. Nation-state cyberattacks become more brazen as authoritarian leaders ramp up aggression. Microsoft, Nov 4. 2022. Available online: https://blogs.microsoft.com/on-the-issues/2022/11/04/microsoft-digital-defense-report-2022-ukraine/

Chirgwin, R. 2017. Fake mobile base stations spreading malware in China. The Register. Available online: https://www.theregister.com/2017/03/23/fake_base_stations_spreading_malware_in_china/

Colman, A.M. 2014. A Dictionary of Psychology (3 ed.) Oxford University Press. ISBN: 9780199534067

DefenceWeb. 2023. SANDF Cyber Command operating in limited space. Available online: https://www.defenceweb.co.za/featured/sandf-cyber-command-operating-in-limited-space/

Hall, S., 2016. *Cyberspace at the operational level: warfighting in all five domains*. Joint Military Operations Department Newport United States.

Hevner, A., Chatterjee, S., Hevner, A. and Chatterjee, S., 2010. Design science research in information systems. *Design research in information systems: theory and practice*, pp.9-22.
https://www.e-ir.info/pdf/43935

Koebler, J. 2015. "The FBI admits it uses fake cell phone towers to track you." Motherboard Tech by Vice. Available from https://www.vice.com/en/article/jp5azg/fbi-admits-it-uses-fake-cell-phone-towers-to-track-you

Litster, G., Hurst, A. and Cardoso, C., 2023. A Systems Thinking Inspired Approach to Understanding Design Activity. In *Design Computing and Cognition'22* (pp. 161-177). Cham: Springer International Publishing.

Mtsweni, J., Gcaza, N. and Thaba, M., 2018, September. A unified cybersecurity framework for complex environments. In Proceedings of the Annual Conference of the South African Institute of Computer Scientists and Information Technologists (pp. 1-9).

Mtsweni, J., 2015. Analysing the security posture of South African websites. In *2015 Information Security for South Africa (ISSA)* (pp. 1-8). IEEE.

NATO. 2022. Cyber Defence. Available Online: https://www.nato.int/cps/en/natohq/topics_78170.htm

Ndebele, l. 2023. US Army to train some African countries in cyber, land and maritime defence. Available from: https://www.news24.com/news24/africa/news/us-army-to-train-some-african-countries-in-cyber-land-and-maritime-defence-20230116. Last Accessed: 01 February 2023

Nigerian Army. 2022. Cyber Warfare Command. Available Online: https://army.mil.ng/?page_id=5714

NIST, 2018. Framework for improving critical infrastructure cybersecurity, version 1.1. Available online: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Oosthuizen, R., & Roodt, J. 2008. Credible Defence Capability: Command and Control at the Core. Land Warfare Conference

Pieterse, H. 2021. The cyber threat landscape in South Africa: A 10-year review. *The African Journal of Information and Communication (AJIC), 28*, 1-21. https://doi.org/10.23962/10539/32213

Samme-Nlar, T. 2020. The future of armed conflict in Africa: what cyber-attacks on Ethiopian government tells us. Available online : https://aanoip.org/the-future-of-armed-conflict-in-africa-what-cyber-attacks-on-ethiopian-government-tell-us/

Shankar, A. 2023. Offensive Cyberspace Operations: using artificial intelligence and kill chains to analyze the effects of MAGTF execution authority. Marine Corps Gazette. February 2023. Available from: https://www.hoover.org/sites/default/files/research/docs/Offensive%20Cyberspace%20Operations%20-%20MCG%20-%20Feb%202023%5B93%5D.pdf

Smith. C and Oosthuizen R, 2012. Applying systems engineering principles towards developing defence capabilities. Available Online: https://incose.onlinelibrary.wiley.com/doi/abs/10.1002/j.2334-5837.2012.tb01383.x?casa_token=W7MQrWozFTAAAAAA%3ANtijJM3-_Wkq1M997uQg4_VEgcKJLZX_tQoZHkJQKDtGL8gVP57gcjvDqKBwQ2nf3XTXrl0F3iuNwCM

South African Government. 2014. South African Defence Review 2014. Available online: https://www.gov.za/sites/default/files/gcis_document/201409/dfencereview2014.pdf

State Security Agency. 2015. The National Cybersecurity Policy Framework (NCPF) for South Africa. Available online: https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf

Tarnowski, I., 2017. How to use cyber kill chain model to build cybersecurity? European Journal of Higher Education IT.

US DOD. 2018. Joint Publication 3-12: Cyber Operations. Available from: https://publicintelligence.net/jcs-cyberspace-operations/

vom Brocke, J., Hevner, A. and Maedche, A., 2020. Introduction to design science research. In *Design science research. Cases* (pp. 1-13). Springer, Cham.

Voo, J; Hemani, I; and Cassidy, D. 2022. National Cyber Power Index 2022. Belfer Center for Science and International Affairs. Harvard Kennedy School. [Online] Available from: https://www.belfercenter.org/publication/national-cyber-power-index-2022, Last Accessed: 01 February 2023

Wang, A. 2023. Cyberwarfare: the final frontier of conflict. Havard Model Congress, Boston, USA. Available from: https://www.harvardmodelcongress.org/s/HMC-2023-Cyberwarfare-dhtw.pdf Last Accessed 01 February 2023

Willers, C. J., Al-Ghamdi, A. A, Bezuidenhout, D. F., and Al-Hosiny, N. M. 2011. "Establishing an infrared measurement and modelling capability," *2011 Saudi International Electronics, Communications and Photonics Conference (SIECPC)*, Riyadh, Saudi Arabia, 2011, pp. 1-6, doi: 10.1109/SIECPC.2011.5876978.