Defining Cyber Warfare Capability Attributes and Characteristics for African Cyber Missions

Mphahlela Thaba
Council for Scientific and Industrial Research (CSIR)
jthaba@csir.co.za

Jabu Mtsweni
Council for Scientific and Industrial Research (CSIR)
mtswenij@gmail.com

Abstract

The domains of warfare have become complex, where cyberspace is declared as the fifth domain. The complexity of cyber space is that it is borderless, and war could be launched from anywhere, and is a serious concern for national security. There is also a different understanding on what cyber warfare needs to entail for nations to be able to defend and/or exploit the cyber space to sustain their territorial integrity and sovereignty. At the same time, the cyber warfare domain is dominated by developed nations, whilst African states are mostly left behind without fully appreciating the comprehensive capabilities (e.g. processes, people, and technologies) required to participate in this arena. This paper extends on the research of the authors in unpacking a comprehensive framework for developing cyber warfare capabilities for African militaries. It unpacks the framework to specific and measurable cyber warfare capability attributes and characteristics, especially for offensive objectives. This could aid African militaries to develop and mature their cyber warfare capabilities over time. This paper also suggests the implementation roadmap, considering all stakeholders and the most efficient way for establishing this strategic and national capability. The significance of the work presented in this paper is that it may aid nation states to systematically develop their cyber warfare capabilities to enable them to participate and/or be ready for participation in the fifth domain of warfare.

1 INTRODUCTION

Forrester Research reported that state-sponsored cyberattacks rose nearly 100% between 2019 and 2022 and their nature changed, with a greater percentage now carried out for data destruction and financial theft [1]. Cyber attacks such as ransomware, spear phishing, cyber terrorism and others are seen as a real threat to national security by many countries. As such many developing countries are building both defensive and offensive capabilities to combat attacks online. The continued attacks in the cyberspace by nations and non-nation actors is becoming a serious challenge for national security [2].

It is therefore evident that modern warfare continues to evolve beyond the traditional domains of warfare including to the cyberspace, due to the technology development in the operational environment [3]. Modern militaries strive to improve their capabilities exploiting all avenues available, to be able to handle the challenges and complexities of the new battlespace. But it is also clear that countries are not at ease with their capabilities in the cyberspace as many are still developing, and this include countries such as the United States, Russia and China [1]. Furthermore, nations have different approaches on how they develop their cyber offensive capabilities, and in most cases what offensive capabilities nations possess is mostly not visible [4].

In addition, the era of defining warfare and associated capabilities along the war domains boundaries is fast ending, due to the integrating nature of the cyberspace [5]. It is also evident through research that many nations, especially in African states are not fully mature when it comes to cyber warfare capabilities and others do not fully understand critical capabilities to have in place to participate in the cyber warfare domain [6], and this is mainly due to the digital divide phenomenon and Africa still mostly focused on socio-economic challenges. And in some cases, African countries have become a pathway or proxies to covert cyber operations amongst the large nations [7].

This paper therefore seeks to help define the cyber warfare capability with specific concentration on the its attributes and characteristics using a strategic framework that may guide nation-states in developing their cyber warfare capabilities following a clear path of implementation.

1.1 TERMS AND DEFINITIONS

It is well known that the dominant nations such as China, Russia, United States, and European states do not define or agree on the terminologies used in the cyberspace and let alone in the cyber warfare domain [8]. For this paper, our goal is not to solve this complex challenge of definitions, but to provide a definition that may aid the reader in understanding our perspective when we define the cyber warfare capability attributes.

In this paper, we define cyber warfare as a capability of a nation-state to exploit another nation-state's cyber-related assets such as communication networks, computer systems and/or other critical information infrastructure for purposes of causing delay, disruption, and/or damage [9]. In addition, cyber warfare capability relates to the ability of a nation, state, or military to conduct operations in the cyberspace. For the military, these operations are meant to defend the country against any aggression within the cyberspace, and/or exploitation of the cyberspace to create freedom of action for own forces through the cyberspace, and/ or beyond to the other domains.

According to Smith and Oosthuizen [10], a capability is defined as the "ability to do" and may be conceived of as comprising nine POSTEDFIT (Personnel, Organisation, Sustainment, Training, Equipment, Doctrine (Policies), Facilities, Information and Technology) constituent elements. Cyber warfare takes effect through a myriad of cyber operations, which 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 [11].

2 CYBER WARFARE CAPABILITY FRAMEWORK

In our paper [12], we proposed a comprehensive capability framework that could be used to establish, deploy, and sustain cyber warfare capabilities. This framework is depicted in Figure 1.

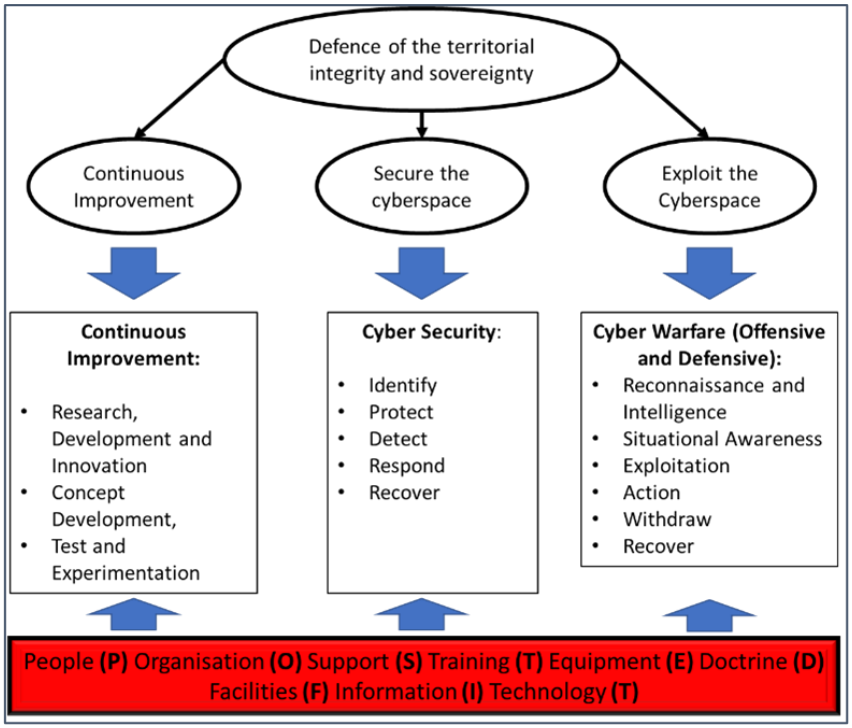

Figure 1: Proposed Comprehensive Cyber Warfare Capability Framework.

The foundation of the framework is the goal of having cyber warfare capability, which is on defending nation's territorial integrity and sovereignty. This goal can be achieved through three key objectives:

- Securing the cyber space,

- Exploiting the cyber space, and
- Continuous capability improvement.

Securing the cyberspace is related to the mandate to defend the country against any threat or risks to its sovereignty. This ability is better defined using the National Institutie of Technology Standards (NIST) framework for Cybersecurity, addressing the following attributes [13]:

- **Identify:** This relates to the ability for a nation to identify and understand their assets in cyberspace, and all its interdependencies.This may include computers, servers, data, intelligence, intellectual property, and people. This also refers to the nation being able to identify its risks and threats that may impact its cyberspace and associated assets.
- **Protect:** This relates to the protection of the assets including the cyberspace, in as far as all its components are concerned. For nation-states, this would also involve the protection of critical information infrastructure as defined by the US Cybersecurity & Infrastructure Security Agency [14].
- **Detect:** This defines the ability of a nation or orgaisations to detect any threats, anomalies, including attempts of intrusion by the adversaries into the cyberspace of the nation and/or into its associated assets.
- **Predict:** In today's cyberspace, reactive responses are not sufficient, and nations need to have the ability to predict cyber attacks against their assets based on threat intelligence so as to respond timely and minimize the damage to its critical assets and operations.
- **Respond:** This relates to the ability to respond to any actions intended against critical assets in the cyberspace by the adversary. This response is often prompted by actions as detected or anticipated.
- **Recover:** This relates to the ability to recover in the instance where adversary actions managed to penetrate and cause damage to the infrastructure or related assets of the nation-state.

The capabilities that a nation needs to have to achieve the objective to secure the cyberspace are set out under each of the objectives supported by the POSTEDFIT elements. As such this paper does not focus on the ability to secure the cyberspace, as the NIST cybersecurity framework as adopted by the authors gives a good basis for this capability, and its development and management.

The *exploitation of the cyberspace* is the main focus in this paper and the attributes/elements of the capability are mostly aligned to this objective. This objective, if well executed, can create freedom of action for own forces, that may span across the other domains of war. The ability of any military to operate and dominate the modern battlespace, has highly become dependent on the ability to exploit the cyberspace. Therefore, developing cyber capabilities, as an integral part of the military capabilities has become more important than ever.

The cyberspace is forever evolving and transforming as new threats and attacks emerge, and as such one of the critical objectives of the comprehensive framework for cyber warfare capabilities is *continuous improvement.* This may include research and development, improvement and/or enhancement of cyber tools, human capacity development, upgrades of doctrines, concept development, tests and experiments, and establishment of efficient means to secure and exploit the cyberspace for purposes of maintaing dominance and/or protection.

In implementing the framework, we proposed a capability matrix that is mapped to capability attributes (functions) and capability elements [12]. The elements were 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 missions under different operational context and requirements. In this conceptual 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.

3 THE CHARACTERISTICS AND ATTRIBUTES OF THE CYBER WARFARE CAPABILITY

Any military capability is characterized by the attributes it provides, and the elements that constitute this capability.

(Thaba and Benade, 2014). Nation-states define these differently, however there is always a common thread among these differing definitions by nations. The basis for military capability, is the ability to achieve military objectives, which is anchored in the ability to conduct military operations. In the physical domains of land, maritime, air, and space, the boundaries are easily identifiable. The cyber space does not have any defined boundaries and exists in all the four domains. The cyber space can be declared as an integrating domain.

Using the attributes of military capabilities as defined in the other domains [15], it can be established that for the cyber warfare capability to achieve the objective of exploiting the cyberspace, the following attributes can be used to specify its dimensions:

- **Effects:** This attribute in cyberspace is related to the ability to cause the desired effect using cyber tools and related. This could relate to destruction, disruption and denial including deception. This attribute represents the ability to project means of causing effect that will impact the ability of the adversary to operate as intended.
- **Mobility:** This relates to the ability to manoeuvre within cyberspace. This relates to the ability to project the cyber capabilities within the space, and all related movement to occupy and conduct operations within the cyberspace. The speed, and agility at which activities can be conducted within cyberspace helps to measure this attribute.
- **Protection:** While projecting capabilities within cyberspace, it is equally important to ensure that they are protected from the adversary. This protection concentrates on the deployed capabilities, and their safety while they conduct operations.
- **Command and Control (C2):** This is the ability to exercise authority over forces operating in cyberspace. This is critical to coordinate activities, which may be difficult especially in a boundary-less domain. Situational Awareness is the critical component of this attribute.
- **Reconnaissance:** Any operation's success is heavily dependent on the intelligence available. Cyberspace is characterized by large data which if not always well understood and process may be threat to operations. On the opposite, if better exploited may enhance operations. This feeds into the Situational Awareness component in C2. The attribute includes the ability to gather data, process and disseminate timely intelligence to the operation.
- **Sustainment:** The success of operations depends on the ability to sustain military forces in operations. This attribute includes the ability to support cyber capabilities in operations. This is critical to the success of any mission, and the plan must be an integral part of the operational plan.

This conceptual research suggests the packaging of these within the attributes as defined using the physical domains related attributes, to standardize on the language used across development, management, and maintenance of current and future military capabilities. Table 1 below depicts this mapping:

Table 1: Cyber Warfare Capability Attributes and Characteristics

GOAL	Capability	Capability Attributes	Capability Characteristics	Objective	Example
Exploitation	**Ability to conduct Offensive and Defensive Cyber Operations**				
		Effects (Cyber power)	Disrupt	Disable the ability to perform as intended	Disable adversary C2 systems Disable Adversary Air Defence Systems to enable Air Strikes
			Destroy	overwriting, erasing, or physically destroying information so that it cannot be recovered	Destroy Adversary HQ Datacentre, or C2 Data, or Destroy Adversary Target Data
			Deny	Make inaccessible to intended users	Encrypt C2 systems, or Log support systems

			Deceive	Create decoys, create wrong targets,	Create wrong Targets on Strategic Weapons, put Adversary own positions as targets.
		Command, Control, communicate and coordinate (C4)	Command and Control	Exercise authority over deployed cyber operations. Control and coordinate deployed forces independently or as part of a joint force by communication	Operate a Command and Control System
			Situational Awareness, Common Operating Picture	Know and understand the deployment of own forces, and the enemy situation (update from intelligence). Ensure same language understood by all deployed and across including as part of Joint Force	Platform or infrastructure to facilitate a common operational picture for the joint force, across all domains
		Manoeuvre	Intrusion and Extrusion	Create freedom of movement withing the adversary cyberspace.	
			Penetration	Provide Access to own forces to the adversary,	
			Stealth	Ensure concealment of all movement as required. Passive Protection	
		Sustain and Support	Keep deployed tools alive Recharge, provide communication etc	Infrastructure required to sustain and support projected forces (actions)	
		Reconnaissance	Reconnaissance: Strategic, Operational	Gather current information or updated about adversary, or adversary environment in the cyberspace in support of Military Strategic objectives	
			Process Intelligence	Collate, process, and Disseminate Create own level Int Picture	

The capability to explore the cyberspace, either in an offensive, or defensive mode will often be an effort combined amongst various stakeholders, private and public due to the boundaryless nature of the cyberspace.

4 A MATURITY ROADMAP FOR CYBER WARFARE CAPABILITY

When building the cyber warfare capability, it is acknowledged that these cannot be built at once. As such cyber warfare capability maturity model or roadmap is required to:

- 1) provide current capability posture of the nation-state,
- 2) benchmark nation-state's warfare capabilities against other nations,
- 3) optimize and prioritize capability investments and development,
- 4) align defensive and offensive capabilities, and
- 5) track, monitor and improve cyber capabilities.

This is purely because several elements influence the development of any capability, and these could be lack of resources

such as people and funding. It is therefore critical that a systematic approach is followed to build the cyber warfare capability with an understanding of interacting socio-technical systems and accepting that "Rome" was not built in a day.

In this section, we therefore suggest a maturity roadmap that could be adopted to build a comprehensive cyber warfare capability encompassing the defined attributes and characteristics. Several cybersecurity maturity models that purport to support the establishment of cyber capabilities exist such as the Cyber Maturity Model Certification (CMMC) by the US Department of Defence [16], NIST Cybersecurity Framework (CSF) [13], and Cybersecurity Capability Maturity Model (C2M2) [17]. However, all these models tend to mostly focus on the defensive side of cybersecurity, and do not deal with cyber warfare capability maturity roadmap.

In this research, we use the comprehensive framework stated in Section 2, and the cyber warfare capability and associated attributes and characteristics to formulate a maturity roadmap that could guide nation-states on how to establish, deploy, improve, and maintain their cyber warfare capabilities.

Capability	Attributes	Characteristics			
Offensive and Defence Cyber Operations	A. Cyber Power	*A.1 Deny*	*A.2 Degrade*	*A.3 Disrupt or Deceive*	*A.4 Destroy*
	B. Command, Control, Communication and Coordinate (C4)	*B.1 Communicate*	*B.2 Command*	*B.3 Control*	*B.4 Coordinate*
	C. Maneuver	*C.1 Evade*	*C.2 Penetrate*	*C.3 Intrusion*	*C.4 Extrusion*
	D. Sustain and Support	*D.1 Monitor*	*D.2 Recharge*	*D.3. Improve*	*D.4 Maintain*
	E. Reconnaissance	*E.1 Observe*	*E.2 Orient*	*E.3.Decide*	*E.4 Act*
Maturity Levels		***Level 1- Basic***	***Level 2 – Intermediate***	***Level 3– Proactive***	***Level 4 – Advanced***
Recommended Roadmap		***1-2 years***	***2-4 years***	***4 – 6 years***	***6 – 8 years***

Figure 2: Cyber Warfare CapabilityMaturity Roadmap

The roadmap can be understood as follows: the capability is the main objective to be achieved, and this capability is associated with desired effects, which we call "attributes" as explained in the previous section.

The five (5) attributes are mapped to characteristics and maturity levels (shown at the bottom of Figure 2 and recommended number of years for development starting from base zero. The roadmap suggests that the nation-states basic (Level 1) cyber warfare capability is defined by the characteristics that are mostly focused on the foundational capabilities. These include observations (E.1) and blocking of attacks (A.1) as examples. A nation state is measured at Level 2 Intermediate if it can deny (A.1) and degrade (A.2) the advisory's cyber power.

Second, the stakeholder is able to communicate (B.1) and command (B.2) in the cyber space, and can to some extent penetrate (C.2) the enemies' environment, but above all is able to orient (E.2.), that is, making informed decisions based on observations made across the whole cyber environment. Level 3 is termed "Proactive" as it does not only focus on capabilities that merely support reaction to situations, but the nation-state is able to disrupt the adversary's actions, deceived the enemy, and improve or decide what to do with the intelligence collected through reconnaissance over and above the capability characteristics found in Level 1 and Level 2. Level 4 is the last maturity level and deals with characteristics that focused on all levels including activities to destroy (A.4), maintain (D.4) and act on the reconnaissance (E.4). The estimated ideal period for a nation state to this level is 6-8 years. It should however be noted that this can be reached earlier depending on the resources and budget of the sponsor.

5 CONCLUSION

This paper defines cyber warfare capability attributes and characteristics for African Cyber Missions. It unpacks the components of the framework to specific and measurable cyber warfare capabilities attributes and characteristics. This could aid African military to develop and mature their cyber warfare abilities over time. The cyber warfare capability framework is described. The characteristics and attributes of the cyber warfare ability are defined. The ability to exploit the cyberspace to create freedom of action for own forces within the cyberspace and across other domains is defined. An implementation roadmap is provided with suggested timelines on how the cyber warfare capability to exploit the cyber

space could be executed over time.

6 REFERENCES

[1] E. Tucker and F. Bajak, "White House cybersecurity strategy stresses software safety," ABC News, 2 March 2023. [Online]. Available: https://abcnews.go.com/Technology/wireStory/biden-administration-releases-new-cybersecurity-strategy-97575586. [Accessed 24 05 2023].

[2] N. Caplan, "Cyber War: the Challenge to National Security," *Global Security Studies,* pp. 93-115, 2013.

[3] S. Hall, "Cyberspace at the Operational Level: Warfighting In All Five Domains," 2016. [Online]. Available: https://apps.dtic.mil/dtic/tr/fulltext/u2/1021506.pdf. [Accessed 1 6 2023].

[4] C. . Trezza, "Negotiation on Cyber Warfare," , 2017. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-319-54975-0_16. [Accessed 1 6 2023].

[5] L. . Natali, "Cyber warfare as chameleonic war: a study of the new ways to conduct war in the 21. century," , 2015. [Online]. Available: https://tesi.eprints.luiss.it/14788. [Accessed 1 6 2023].

[6] U. M. Mbanaso, "Cyber warfare: African research must address emerging reality," *South African Journal of Information and Communication,* vol. , no. 18, p. 0, 2016.

[7] J. . Kallberg and S. . Rowlen, "African nations as proxies in covert cyber operations," *African Security Review,* vol. 23, no. 3, pp. 307-311, 2014.

[8] A. A. Galushkin, "Theoretical and legal aspects of cyber warfare," *Mediterranean journal of social sciences,* vol. 7, no. 1, pp. 570-573, 2015.

[9] A. Wang, "Cyberwarfare: the final frontier of conflict.," Harvard, 2023. [Online]. Available: https://www.harvardmodelcongress.org/s/HMC-2023-Cyberwarfare-dhtw.pdf. [Accessed 1 February 2023].

[10] C. Smith and R. Oosthuizen, "Applying systems engineering principles towards developing defence capabilities," in *INCOSE Conference*, 2012.

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

[12] M. Thaba and J. Mtsweni, "Developing Robust Cyber Warfare Capabilities for the African Battlespace," in *22nd European Conference on Cyber Warfare and Security*, Athens, Greece, 2023.

[13] NIST, "NIST Cybersecurity Framework," National Institute of Standards and Technology, 2023. [Online]. Available: https://www.nist.gov/cyberframework. [Accessed 01 June 2023].

[14] CISA, "Critical Infrastructure Sectors," 2022. [Online]. Available: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors. [Accessed May 2023].

[15] M. Thaba, J. Mtsweni, M. Molekoa and A. Mxoli, "Developing Cyber Warafe Capabilities as an Integral Part of Command and Control," in *24th International Command and Control Research and Technology Symposium*, Laurel/Maryland, USA, 2018.

[16] AustCyber, "United States Government's Cyber Security Maturity Model Certification," 2020. [Online]. Available: https://www.austcyber.com/news-events/united-states-governments-cyber-security-maturity-model-certification. [Accessed 02 February 2023].

[17] HC3, "HHS Cybersecurity Program," 2020. [Online]. Available: https://www.hhs.gov/sites/default/files/cybersecurity-maturity-model.pdf. [Accessed 05 February 2023].