Cyber Power in the African Context: An Exploratory Analysis and Proposition

Petrus Duvenage, Wilhelm Bernhardt and Sebastian von Solms
University of Johannesburg, South Africa

duvenage@live.co.za
wbernhardt@vodamail.co.za
basievs@uj.ac.za

Abstract: While the centrality of cyber power in the safeguarding and advancing nation states' national interests and objectives is now widely accepted, the academic discourse (on cyber power) is still incipient. In literature reviewed, cyber power is predominantly viewed as comprising of two dimensions, namely offensive and defensive. The exploratory analysis we conducted found that Africa's unique, contextual factors necessitate an expanded conceptualisation of cyber power. This alternative conceptualisation does not dispute the existing notion that cyber power has offensive and defensive dimensions. The fact that cyber is by its very nature borderless and that African countries function in an interconnected global arena of competition and conflict, are also not contested. What is required is the addition of a third dimension to cyber power, namely developmental power. This paper advances a tentative proposition on a cyber-power triad (with offensive, defensive and developmental dimensions). This proposition, we argue, is more apposite to African countries' national objectives —strategically and in the allocation of resources. At least on a notional level, the cyber-power triad can guide the leveraging of the asymmetric advantages that cyber space offers African nation states and in a manner that pursues all three (cyber power) dimensions in a complementary manner. Such synergetic wielding of cyber power is one of the keys indispensable to African countries addressing their substantial challenges and unlocking their vast potential.

Keywords: Cyberpower, Nation States, Developing Countries, Cyber Power Model, Cyber Power Index, Global South.

1. Introduction

It is projected that Africa's population will double as early as 2050, characterised by a sizeable youth bulge. In fact, according to the World Economic Forum (WEF), by 2030, young Africans are expected to constitute 42% of global youth (El Habti, 2022). The political and economic implications of this trend are multiple, and of considerable impact. On the one hand, it raises fears of burgeoning unemployment, rising poverty and pervasive conflict, whilst on the other there is tremendous potential for economic development and mounting political influence, not only on the continent, but on a global scale. The African Union's (AU) Digital Transformation Strategy for Africa (2020 – 2030) acknowledges these projections, and notes that 'digital transformation' is a driving force for sustainable growth (AU, 2020). It envisages an integrated and inclusive digital society and economy in Africa that improves the quality of life of Africa's citizens, strengthen the existing economic sector, enable its diversification and development, and ensure continental ownership with Africa as a producer and not only a consumer in the global economy (AU, 2020). It is therefore not surprising that the optimal utilisation of cyberspace features prominently as an enabling force in the AU's 'Agenda 2063', promoted as Africa's "blueprint ...for transforming Africa into the global powerhouse of the future" (AU, 2015). Optimising the utilisation of cyber space, in turn, and as this paper will show, has as prerequisite a fit-for-purpose conceptualisation of cyber power.

The academic discourse on cyber power is in various respects still incipient and evolving (Cavelty, 2018; BAE, 2022). At least in as far as consultant literature is concerned, 'cyber power' emerged as a distinctive concept in the United States (US) early in the first decade of the 21st century, but only gained wider academic traction from 2009 onward (Starr, 2009; Cavelety, 2018). The limited academic literature that has subsequently been advanced is overwhelmingly predisposed directed to the Global North. (The 'Global North', when used in this paper denotes the Western world and other developed economies, including Japan and Israel. The Global South largely corresponds with developing countries in Africa, Latin America and the East (Pagel *et al,* 2014).

While there are differences, the limited literature on cyber power mostly reflects Global North commonalities in approach and assumptions. Unsurprisingly, this literature is predisposed towards the national objectives of the Global North's powerful states and that of their major adversaries. Accordingly, cyber power was, and for a

substantial part is still, analysed in the context of inter-state conflict, specifically in relation to economic and especially military type antagonism and rivalry. As recently as 2018, the Global North's conceptualisation of cyber power predominantly remained one dimensional, namely 'offensive' (Cavelty, 2018). Of late, however, there is growing acceptance that 'cyber power' has an integral second dimension, namely defensive power. In the Global North's view this sum of an actor's offensive and defensive cyber power is relative to those of others (Devanny, Goldonia and Medeiros, 2022). There is thus a hierarchal distinction to be made between actors with more, lesser or equal cyber power.

Even in comparison with the limited (but expanding) Global North literature, peer-reviewed academic contributions which specifically explores cyber power within the context of sovereign states located towards the lower end of the international spectrum of national power, is scarce (van Niekerk, 2019). More often than not, cyber power concepts and indices from the Global North are applied practically without qualification to the Global South in general, and Africa in particular.

Herein lies the glitch - as with other forms of power, conceptualisations of cyber power are context specific and cannot necessarily be applied unchanged (if at all) to other polities (Cavelty, 2018). Subsequently, this paper poses the following questions:

- What, in more detail than outlined above, is the Global North's mainstream view of cyber power?
- How pertinent and applicable is the global North's conceptualisation of cyber power to the global South in general, and Africa in particular?
- Is there a need for an expanded or alternative conceptualisation of cyber power?
- If indeed required, what contextual factors should be considered should in shaping an African specific conceptualisation?
- Albeit tentative, what proposition on cyber power apposite can be advanced?
- What are the implications of an alternative proposition for the assessment of cyber power in Africa?

This paper's central contention is that Africa's unique, contextual factors necessitates an alternative conceptualisation of cyber power, which should be more inclusive, holistic, and incorporate not only the ability to defend the state's interests, and/or to influence or attack an adversary with cyber instruments, but critically also a third dimension: the capacity to optimise the state's development policies. Thus, we advance a tentative proposition on a cyber-power triad (with offensive, defensive and developmental dimensions). This proposition, we argue, is more relevant to African countries' strategic national objectives. At least on a notional level, the cyber-power triad can guide the leveraging of the asymmetric advantages that cyber space offer African nation states and in a manner that pursues all three (cyber power) dimensions in a complementary manner. In this way the relatively limited resources and capacity of African countries can be optimised.

This paper is categorically qualified as an exploratory examination and tentative proposition. It is the first of a series of papers flowing from research at the University of Johannesburg (UJ) on the topic of cyber power in the Africa context. This being the first paper, we endeavour to lay a notional foundation that is being concretised in follow-up research.

Structurally, the paper is aligned with the research questions and consists of the following:

- Section 2 provides an overview of the predominating conceptualisation of cyber power in the Global North.
- Section 3 examines the imperative of developing an expanded proposition on cyber power.
- Section 4 identifies the factors to be considered in formulating a proposition on African cyber power.
- Section 5 advances an African cyber-power triad as a tentative proposal.
- Section 6 examines the implications of this proposal on assessing cyber power in Africa.
- Section 7 concludes the paper by outlining ongoing research on this topic.

2. The Global North's conceptualisation of cyber power

Within the context of international relations, cyber power can broadly be defined as that element of national power aimed at protecting and advancing national interests through and in cyberspace (Devanny 2021; Voo, Hemani and Cassidy 2022). Because this definition is so broad, it is, for all intents and purposes 'compatible' with all works consulted for purposes of this paper.

However, it is on moving from this broad definition to more specific and granulated conceptualisations of cyber power, that views diverge. It is beyond the scope of this paper to dissect these variations. The aim here is to outline the Global North's dominant view of cyber power in the academic discourse. This view is, for a large part, articulated in literature from Western countries. Although it admittedly risks oversimplification, for our purposes here, the Global North essentially views cyber power as comprising of two dimensions, namely the 'offensive' (wielding of power) and the defensive (cybersecurity and resilience). The said two dimensions are further explained in subsections 2.1 and 2.2. This is followed by a concise overview of current cyber power indices, predicated on these dimensions (Subsection 2.3).

2.1 'Offensive' dimension

This Global North's dominant view posits cyber power as an integral part of a nation state's power contestation with other states and non-state actors (Nye 2010). Cyber power is seen both as a dimension of state power and the 5th domain of warfare (in addition to land, sea, air and space). Cyber power is furthermore asserted as cutting across, all *four elements* of national power (Political/Diplomatic, Information, Military and Economic) (Kuehl 2009). As national power in general, cyber power is key to gaining an advantage over competing actors and influencing the environment (Sheldon, 2011). This is achieved through a combined application of coercion ('hard power') and persuasion ('soft power'). Soft and hard power are not exclusive 'categories' but rather comprises a continuum of overlapping aspects ranging from diplomacy and intelligence gathering, to cyber weapons (Van der Waag-Cowling 2019; Devanny, Goldoni & Medeiros, 2022). Used in unison, soft and hard power constitute smart power'. We note that, in a narrow definitional sense, the 'wielding' if cyber power is not always of an 'offensive' nature. 'Offensive' as used here involves more than cyber war /disruptions and also includes influencing, intelligence gathering and surveillance. In fact, "mature offensive cyber capability" includes "intelligence collection and analysis" (Devanny, Goldoni and Medeiros, 2022), as well as cyber counterintelligence (CCI). The latter in turn includes substantial defensive facets (Duvenage, 2019).

2.2 'Defensive' dimension

Cavelty (2018) rightly points out that the Global North's discourse was until very recently all about the offensive domination of one actor over others– be it through hard and/or soft power. Cyber power was thus up to 2018 mainly a one-dimensional construct. One notable exception has been Klimburg's model (2011), which:

> "[Takes] cyberpower out of the context of projecting national interests coercively and adds a strong defensive cyber-security element, built on a best-practice model of cyber-security policy. Such a view highlights that cyberpower and cyber-security are intricately linked. ***A political entity possesses cyber-power if it has the ability to shape aspects of the global cyber-security landscape***. However, a cyber-power also needs to be able to 'defend' against cyber-threats, or rather, manage them adequately. These necessities, internal cyber-resilience and external cyber-power, build on each other: in this view, there cannot be any true cyber-power without cyber-resilience – and vice versa." (Cavelty, 2018 - emphasis added)

Currently, cybersecurity is no longer viewed as complimentary to, but as an integral second dimension of, cyber power. Also this dimension emphasises the importance of projecting power globally. This two-dimensional view of cyber power is clearly reflected in Global-North instruments that aim at measuring cyber power. These instruments are discussed in the next subsection.

2.3 Relative nature of cyber power

As was noted earlier, the Global North posits cyber power as hierarchal and relative. Respective nation states thus possess more, less or roughly equal degrees of cyber power. Since cyber power is relativistic and relational (Devanny, Goldoni and Medeiros, 2022) distinctions are made between cyber super powers, major powers and lesser role-players (Segal, 2016).

Several instruments (models and indices) exist for assessing cybersecurity. Some of these, such as the Global Cybersecurity Index of the International Telecommunication Union (ITU, 2021a) and the University of Oxford (2021) Cyber Security Capacity Centre's Cybersecurity Capacity Maturity Model for Nations (2021) are well-established, have been applied for several years and have wide global coverage. Literature reviewed, however, identified only two current instruments that assesses cyber power (in its offensive and defensive dimensions), namely the Harvard's Belfer Center for Science and International Affairs index (Voo, Hemani and Cassidy, 2022)

and the United Kingdom-based International Institute for Strategic Studies assessment model (IISSS 2021). Read in conjunction with the BAE's (2022)"hallmarks" of a leading cyber power, these instruments clearly reflects the key contentions of the Global North's view on cyber with power: in order to be a major player a nation state has to project cyber power with a global reach – offensively and defensively. In tabulated format, the measuring criteria employed are as follows:

Table 1: Comparative assessment of cyber power

	Belfer Center	International Institute for Strategic Studies	BAE
Metho-dology	• Quantitative and qualitative	• Quantitative	• Qualitative
Aspects	• Surveilling and Monitoring Domestic Groups • Strengthening and Enhancing National Cyber Defenses • Controlling and Manipulating the Information Environment • Foreign Intelligence Collection for National Security • Growing National Cyber and Commercial Technology Competence • Destroying or Disabling an Adversary's Infrastructure and Capabilities • Defining International Cyber Norms and Technical Standards • Amassing Wealth and/or Extracting Cryptocurrency	• Strategy and doctrine • Governance, command and control • Core cyber-intelligence capability • Cyber empowerment and dependence • Cyber security and resilience • Global leadership in cyberspace affairs • Offensive cyber capability	• Power projection through showing international leadership in national cyber defence capabilities, supported by the cyber defence ecosystem. • A clear and holistic cyber strategy for the nation, led by a strong national cyber agency co-opting all parts of government, industry and society. • A strong technology sector that drives prosperity, enables and contributes to national cyber defences, and is capable of exporting cybersecurity capabilities. • Effective collaboration between government and the technology sector, to influence the evolution of tehnology and standards. • A clearly articulated vision for the future of the internet that embodies the values of government and society. • Cyber diplomacy and relationship-building – the ability to show leadership and promote its vision for norms and values in and through cyberspace. • Responsible development of and use of offensive cyber capabilities.

Sources: Voo, Hemani and Cassidy, 2022; IISS, 2021; BAE, 2022 [Verbatim].

The afore-mentioned instruments are far more selective than the ITU (2021a) and Oxford (2021) cyber security indices with the IISS (2021) assessing 15 and the Belfer Center 30 nation states respectively (Voo, Hemani and Cassidy (2022). Overall, these cyber power assessment instruments find the world's major and superpowers as aspiring to an exceptional degree of offensive and defensive cyber power to achieve their global ambitions and influence. Therefore, such nation states are regularly accorded high rankings.

No African nation state features in the IISS (2021) assessment, while the Belfer Center ranks Egypt as 24th out of 30 countries (Voo, Hemani and Cassidy, 2022). While both these instruments admit limitations, both are commendable in appraising cyber power; ***if*** (i) cyber power is deemed as only having two dimensions – offensive and defensive; and (ii) a nation state aspires to substantially extend its global reach. As will be elaborated upon in the next section, not all nation states have such aspirations and are more focused on pursuing strategies in which 'internal/domestic' national interests dominate. This raises the question of the strategic usefulness of the two-dimensional cyber power construct in the broader setting of less well-resourced nation state's national power, national security and national interests.

3. The imperative of developing an expanded conceptualisation of cyber power

A recent comprehensive study conducted by Çifci (2022) developed a conceptual framework for the comparison of 11 cyber power and cyber security indices. Çifci (2022: 10) rightly asserts that "cybersecurity and cyber power indices, do not necessarily have to be the same or universally accepted. Every individual or organization has their own views on these concepts." The context-specific qualification does of course not distract from the value of

current national-level cybersecurity capability assessments in informing the bolstering of defensive cyber power. Neither does it dispute the insights offered by current assessments of offensive cyber power.

However, since cyber power is contex-specific it needs to be asked whether outside the Global North (i) the construct of cyber power as having two dimensions (offensive and defensive) is sufficient; and (ii) to what degree global aspirations should universally be a major criterion for assessing cyber power? Is it analytically credible to, for a significant part, measure cyber power as states' ability to establish control and exert influence over adversaries within and through cyber space, as though the control and influence are objectives in themselves? Furthermore, whilst it may make strategic sense for some Global North states to develop a vast national capacity of which the sole aims are cyber disruption, cyber espionage, and cyber degradations as the means to influence a rival actor (Valeriano *et al* 2018), for others, with different or less adversarial national objectives, this would actually amount to a strategic misalignment of resources.

The vast majority of African states - the world's 'minor powers' from a national power point of view - generally do not reflect similar levels of global aspirations. The national objectives of such states, and their applications of national power, in fact tend to be located much closer to home, at the intra-state level, and directed towards efforts aimed at eradicating or alleviating poverty by means of development programmes (Odeh, 2010). Development, in this sense, essentially refers to the process through which a country increases its capacity to meet its citizens' basic human needs and raise their standard of living (Kegley and Wittkopf, 1999). Does this emphasis on development imply that cyber power is of lesser strategic importance to African states? Does cyber power mean the same to these states as it does to the Global North?

It is the contention of this paper that African states have unique national objectives that are not a mirror image of those of the world's super and major powers. However, this certainly does not imply Africa is irrelevant from a cyber-power perspective, and only become relevant from the perspective of cyber power indices when and if they pursue cyber power on the same terms as the world's major and superpowers. It is consequently proposed that questions regarding the relative cyber power of the world's nations should be also approached from a complementary perspective, *viz*.: *whether the extent of cyber power at any state's disposal is properly aligned to and sufficient to address that particular state's unique combination of national objectives?* To achieve this, an expanded proposition of cyber power which considers the African context, is required.

4. Context for the conceptualisation of an African cyber power construct

Elaborating on Section 3, this section discusses in more detail the contextual factors that will shape an expanded conceptualisation of cyber power apposite to Africa.

4.1 Political and socio-economical context

States that identify with the Global South are located outside Europe and North America, and mostly tend to be low- to middle-income countries, who are in the process of industrialisation, and are frequently former subjects of colonialism (Pagel *et al,* 2014). All nation states on the African continent are thus categorised as part of the Global South. As the Global South in general, African countries is likely to be disadvantaged in two distinct ways: firstly, in terms of their relative national power deficits *vis-à-vis* the world's more advanced and powerful states; and secondly with respect to their comparative lower levels of socio-economic and political advancement.

From a **national power perspective** African, the respective nation states cannot achieve security in the international arena by relying only on their own capabilities alone, and prefer policies of neutrality or alliances; do not have the necessary military power to project power on a global scale; and favour a high degree of participation in and support for international organisations, where they pursue 'moral' or 'normative' policy positions, and encourage formal rules in order to curb the great powers and strengthen their own position. These states often display risk averse behaviour in international politics, due to the risk of punitive reprisal should they challenge more powerful states; whilst their geographic demands are predominantly restricted to their own and immediately adjacent areas (Toje, 2010). Their overall behaviour in their interaction with other states are in the main characterised by a general and continuing reluctance to coerce and a tendency to promote multilateral, non-military solutions to security challenges (*cf* Fox, 1959). African states are more likely to be embroiled in military or diplomatic concerns about, or conflict with, their immediate neighbours, instability in the region, and troubles somewhere on the continent. Africa also contains stats that are considered fragile, failing or failed, implying that the continuity of the state can, be at risk from internal, domestic threats such as

civil war, revolutions, or insurrections. These countries are generally also far more likely to experience high frequency social instability, violent protests and unrest as well deep-seated ethnic or racial divisions. Overall, they are likely to be significantly vulnerable to erosion of the state's monopoly on violence – a risk that is less unlikely to occur in the major powers. The establishment of a domestic security and intelligence capacity to counter such phenomena, or to collect information about them locally and abroad – also in cyberspace – should therefore make as much strategic sense to the world's minor powers, as it does for their stronger counterparts. Cyberspace has indeed in this respect: *"ma[d]e it easier to subvert and harder to govern*" (Betz and Stevens, 2011).

From a **socio-economic and political development perspective** African states more often than not tend to experience significant developmental challenges that are not normally associated with more powerful, advanced states. As pointed out by Dados and Connel (2012), the 'Global South', of which Africa is an integral part, is more than a metaphor for underdevelopment, as it actually references: "...an entire history of colonialism, neo-imperialism, and differential economic and social change through which large inequalities in living standards, life expectancy, and access to resources are maintained". In the main, the national objectives of African states are not dominated by globally oriented security concerns. Instead, a sizeable part of such states' national power is directed inward, towards intra-state objectives, such as the development and prosperity of the state; the expansion of its economy; the delivery of basic services to all citizens; anti-crime and corruption measures, as well as the institutionalisation and projection of its national values, nation-building and social cohesion.

Probably the most outstanding characteristic of African nation states in the global context is their national power deficit. As will be substantiated in Sections 5 and 6, cyber space offers asymmetric advantages to more effectively address political and socio-economic priorities and concurrently narrow national power deficits. A proposition on leveraging of cyber space's asymmetric advantages also needs to consider African cyber capacity, challenges and constraints. These aspects are overviewed briefly in the next section.

4.2 Cyber context: Potential, capacity, challenges and constraints

African cyber capacity, challenges and constraints are addressed rather comprehensively in subsequent research that follows this paper (see Section 7). Therefore, we suffice here with the following concise, bulleted overview:

- Although there is a wide variance between countries in respect of cyber capacity and maturity, Africa's vast cyber potential is unfolding (AU 2015; AU 2020). The continent has more than 500 million Internet users – putting it ahead of regions such as North America, South America, and the Middle East (Interpol 2021). While it is underserved in terms of Internet coverage capacity and bandwidth speed, Africa has the fastest-growing telephone and Internet networks globally (Interpol 2021).
- The vast majority of African countries are still in early the early stages of transforming to digital economies (AU 2015; AU 2020: ITU 2021b). Concurrently, there is low self-sufficiency in technological innovation and development (Van der Waag-Cowling, 2019).
- From a defensive perspective, most African countries' cybersecurity and resilience are alarming weak in comparison to other continents. The ITU (2021a) for one, assesses African counties overall as the least committed to cybersecurity. Moreover, leadership in respect of collective defence and security, by bodies such as the AU, is weak (Van der Waag-Cowling, 2019).
- Africa is highly targeted by cybercriminals who perceives it to be the "soft underbelly" of global business networks (McCarthy, 2022). Simultaneously, Africa does not escape targeting by state-sponsored Advanced Persistent Threat (APT) actors (Allen and van der Waag-Cowling, 2021).
- The immature offensive capacity that does exist, relies on imported tools and the outsourcing of functions/services. Overall cyber warfare is not "viewed as priority" (Van der Waag-Cowling, 2019). However, several African countries are known to have vendor-sourced cyber espionage and surveillance capacity that can be deployed domestically and externally (Allen and La Lime, 2021).
- Even if measured against very modest foreign policy aims, African countries' cyber diplomacy effort are inadequate (Van der Waag-Cowling, 2019).

African counties are thus faced with a combination of, on the one hand, political and social-economic challenges and, on the other hand, significant cyber constraints. For cyber power to make strategic sense for such states, it must enable them to achieve **asymmetrical advantages** in the context of their national objectives. Asymmetry, in its use here, refers to the ability of a state to enhance or augment any component of its national power through the strategic application of cyber power, in order to gain specific advantages. Practically speaking, it is

thus about the use of cyber power in a manner that achieves **a force multiplication, or the resource optimisation effect**. A tentative postulation on a cyber-power triad providing a theoretical premise for such power optimisation is advanced in the next section.

5. Tentative postulation on African cyber power triad

Our tentative postulation on African cyber power that would enable optimising resources in levering asymmetric advantages, is depicted in Figure 1. This proposition, which is unpinned by the African-specific context provided in Section 4, is holistic in the sense that it encapsulates three forms of cyber power, namely:

- **Dimension 1**: **Offensive cyber power** that (in its loose connotation) refers not only to the capacity to wage cyber war and disrupt, but also the state's ability to utilise cyber means for influencing, intelligence gathering and surveillance. Although 'cyber war is not a priority to most on the continent, the national security of all African countries demands capacity for surveillance and intelligence gathering.
- **Dimension 2: Defensive cyber power,** since the ability to safeguard cyber-related national assets ought to be an indispensable and integral component of cyber power of all African countries – regardless of economic size and the level of digital development.
- **Dimension 3: Developmental cyber power**, which denotes the capacity to pursue national developmental objectives in cyberspace (in a manner that is in tandem and synergy with the defensive and offensive dimensions).

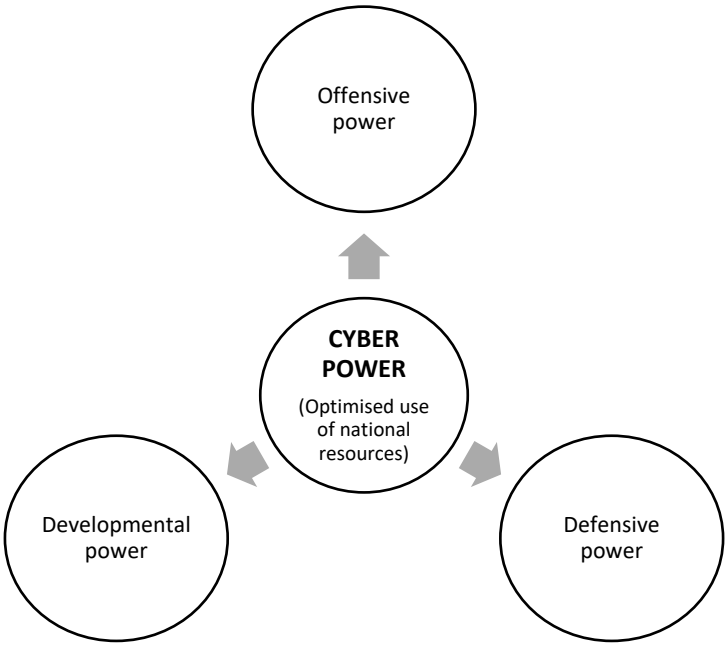

Figure 1: A cyber-power triad for application in the African context

In contrast to cyber power's offensive and defensive dimensions, the paper showed the developmental power dimension as practically unexplored in academic literature (see Sections 2 and 3). As was noted in the introduction, this paper is of an exploratory nature and advances only a tentative proposition. Further work aimed at a substantiated proposal on the developmental cyber power dimension is earmarked for subsequent research (see Section 7). Nevertheless, the following **tentative and preliminary postulations on developmental cyber power** are required to support this paper's contention on the conceptual credibility of a cyber-power triad:

- Developmental cyber power, in its broader connotation, is about a country's collective cyber capacity that is relevant, or potentially relevant, to its national developmental priorities. This capacity has human, institutional, technical and infrastructural facets.

- Like the offensive and defensive dimensions, developmental cyber power depends on appropriate national strategy objectives and measures as well as the allocation of national resources and effort. Given limitations in national resources, African countries have to optimise scarce resources. Therefore, resources can not be devoted to developmental power exclusively. Optimising cyber power requires resources to be shared, and as far as possible serve all three cyber-power dimensions.
- Defensive and offensive cyber power dimensions are essential to support the developmental dimension and *vice versa*.

This section provided a high-level outline of our exploratory postulation on a cyber-power triad for Africa. The next section examines the tentative implications of utilising the cyber-power triad as the core of a qualitative (cyber power) assessment framework.

6. Tentative implications of the cyber-power triad as the core of qualitative assessment framework

The qualitative assessment framework to be designed around the cyber-power triad is predicated on our contentions on national power in Sections 3 and 4. To recapitulate: the national power of states are not equal, their national objectives differ, and therefore their cyber power requirements and strategies should be unique. What works for a superpower as far as national and cyber power are concerned, will most likely not be a usable blueprint for an African country. Therefore, our envisaged approach to assess cyber power is holistic in the sense that it encapsulates all three forms of cyber power and can be applied to evaluate any state in Africa on an equal basis.

Instead of measuring and ranking states in accordance with a presumed hierarchy of greater and lesser cyber powers, the purpose of the holistic assessment would be to ascertain whether any given nation's cyber power is optimally configured to reflect that individual state's cyber power requirements – in other words, whether the state has the ability to do something strategically useful in cyberspace (Gray, 2013). The result of the assessment will be a cyber-power profile, rather than a hierarchical, comparative 'ranking' of states. In this manner, states that require only limited offensive cyber power, are not 'penalised' or relegated to perpetual low positions on a cyber-power index. Our profiling of cyber power would not ask how 'high' a state 'ranks' in relation to the cyber power other states, but rather whether any particular nation's overall national cyber power configuration is appropriately configured to serve that specific nation's unique national objectives, and in which respects it differs from any other state/s.

7. Conclusion

This paper conducted an exploratory analysis of cyber power in the African context.The analysis established the need for an expanded construct in the form of a cyber-power triad (comprising of offensive, defensive and developmental dimensions) and a tentative proposition was advanced on a notional ('abstract') level. This notional construct of a cyber-power triad is subject to, and will be concretised in, further research. It will culminate in the design and application of a qualitative framework for assessing cyber power of African countries. In sequential order, the sub-themes of the envisaged further research items are as follow:

- The African cyber power triad – concretising the developmental dimension.
- A high-level overview of an integrated framework for assessing cyber power in Africa.
- Cyber power in Africa: configuring capacity, challenges and constraints.
- A qualitative assessment of South Africa's cyber power.
- A comparative assessment of cyber power in the Southern African Development Community (SADC) region.
- Cyber power in sub-Saharan Africa: proposal on the cooperation agenda.

Albeit theoretical and academic, we expect qualitative assessments of this nature to be useful in informing African countries' leveraging of the asymmetric advantages that cyber space offer: offensively, defensively and developmental. Although not a panacea, such a synergetic wielding of cyber power is one of the keys indispensable to African countries addressing their substantial challenges and unlocking their vast potential.

References

African Union. 2015. *Flagship Projects of Agenda 2063*. As accessed on 16 January 2023 at https://au.int/agenda2063/flagship-projects.

African Union. 2020. *The digital transformation strategy for Africa (2020-2030)*. As accessed on 16 January 2023 at https://au.int/sites/default/files/documents/38507-doc-dts-english.pdf.

Allen, N. and La Lime, M. 2021. *How digital espionage tools exacerbate authoritarianism across Africa?* As accessed on 11 December 2022 at https://www.brookings.edu/techstream/how-digital-espionage-tools-exacerbate-authoritarianism-across-africa/

Allen, N. and van der Waag-Cowling N. 2021. *How African states can tackle state-backed cyber threats.* Brookings Techstream. As accessed on 09 December 2022 at https://www.brookings.edu/techstream/how-african-states-can-tackle-state-backed-cyber-threats/.

BAE Systems. 2022. *What is cyberpower*. Accessed on 27 November 2022 at https://www.baesystems.com/en/cybersecurity/feature/responsible-cyber-power.

Betz, D. and Stevens, T. 2011. *Cyberspace and the State. Toward a Strategy for Cyber-power*. London: International Institute for Strategic Studies.

Cavelty. M. D. 2018. 'Europe's cyber-power', *European Politics and Society*, vol. 19, nr 3: 304-320, DOI: 10.1080/23745118.2018.1430718

Dados, N. and Connel, R. 2012. *The Global South*. In Contexts, Vol. 11, No. 1, pp. 12-13. https://journals.sagepub.com/doi/pdf/10.1177/1536504212436479.

Devanny, J. 2021. *The Review and Responsible, Democratic Cyber Power*. As accessed on 11 December 2022 at https://www.kcl.ac.uk/the-review-and-responsible-democratic-cyber-power

Devanny, J., Goldoni, L and Medeiros, B. 2022. 'The rise of cyber power in Brazil' in *Revista Brasileira de Politica Internacional*, Vol 65, no 1. DOI: https://doi.org/10.1590/0034-7329202200113.

Duvenage, P.C. 2019. *A conceptual framework for cyber counterintelligence*, unpublished PhD thesis, University of Johannesburg, South Africa.

Çifci, H. 2022. *Comparison of National-Level Cybersecurity and Cyber Power Indices: A Conceptual Framework*. Istanbul: Istanbul Aydin University.

El Habti, H. 2022. *Why Africa's youth hold the key to its development potential*. World Economic Forum. As accessed on 16 January 2023 at https://www.weforum.org/agenda/2022/09/why-africa-youth-key-development-potential/

Fox, A.B. 1959. *The Power of Small States: Diplomacy in World War Two*. Cambridge: Cambridge University Press.

Gray, C.S. 2013. *Making Strategic Sense of Cyber Power: Why the Sky is not Falling*. Carlisle, PA: Strategic Studies Institute

Handler, S. 2021. *The 5×5—Cyber capacity and conflict in Africa*, Atlantic Council. Accessed on 29 November 2022 at https://www.atlanticcouncil.org/commentary/the-5x5-cyber-capacity-and-conflict-in-africa/

International Institute for Strategic Studies (IISSS). 2021. *Cyber Capabilities and National Power: Net Assessmen*t As accessed on 21 November 2022 at https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power 2021)

International Telecommunication Union (ITU). 2021a. *Global Cybersecurity Index 2020*. Accessed on 27 October 2021 at https://www.itu.int/epublications/publication/global-cybersecurity-index-2020/en/.

International Telecommunication Union (ITU) (2021b), *Information and communication technology trends and developments in the Africa region. 2017-2020.* Accessed on 11 September 2022 at https://www.itu.int/pub/D-IND-DIG_TRENDS_AFR.01-2021.

Interpol. 2021. *The African Cyberthreat Assessment Report 2021*. Accessed on 09 December 2021 at https://www.interpol.int/content/download/16759/file/AfricanCyberthreatAssessment_ENGLISH.pdf.

Kegley, C.W. and Wittkopf, E.R. 1999*. World Politics: Trend and Transformation*. World Publishers: New York.

McCarthy, S. 2022. 'Africa needs to improve cybersecurity to boost investment', *World Economic Forum Opinion*. Accessed on 04 November 2022 at https://www.weforum.org/agenda/2022/08/africa-must-act-to-address-cybersecurity-threats.

Nye, J.S. 2010. *Cyber Power*. Cambridge, MA. Belfer Center for Science and International Affairs.

Odeh, L. E. 2010.' A Comparative Analysis of Global North and Global South Economies'. In *Journal of Sustainable Development in Africa* (Volume 12, No.3, 2010). Clarion, Pennsylvania. Clarion University of Pennsylvania.

Oxford Global Cybersecurity Centre: *Cybersecurity Capacity Maturity Model for Nations (CMM).* 2021. As accessed on 13 January 2022 at https://gcscc.ox.ac.uk/the-cmm.

Pagel, H., Ranke, K., Hempel, F. and Köhler, J. 2014. 'The Use of the Concept 'Global South'' in *Social Science & Humanities.* Berlin. Institut für Asien- & Afrikawissenschaften.

Segal, A. 2016. *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Era.* New York, NY: Public Affairs.

Sheldon, J.B. 2011*. 'Deciphering Cyberpower: Strategic Purpose in Peace and War.'* In Strategic *Studies Quarterly*, Vol. 5 No. 2 (Summer 2011), pp. 95 – 112.

Spade, J.M. 2012. *Information as Power. China's Cyber Power and America's National Interest*. Carlisle, PA: US Army War College.

Starr, S.H. 2009. *Towards an Evolving Theory of Cyberpower*. Center for Technology and National Security Policy (CTNSP), National Defense University (NDU). United States.

Toje, A. 2010. *'The European Union as a Small Power.'* In *Journal of Common Market Studies*. Vol 49 (1).

Valeriano, B., Jensen, B and Maness, R.C. 2018. *Cyber Strategy: The Evolving Character of Power and Coercion*. New York: Oxford University Press.

van der Waag-Cowling, N.2019. 'Africa must harness the potential of Cyber Power and Digital Diplomacy' in Very, F (ed.) *Research Brief* 11/2019, Security Institute for Governance and Leadership in Africa, University of Stellenbosch.

van Niekerk, B. 2019. 'The Cyber Security Dilemma: A South African Perspective.' *Proceedings of the 14t^{h} International Conference on Cyber Warfare and Security,* University of Stellenbosch, South Africa .

Venables, A., Shaikh, S.A., and Shuttleworth, J. 2015. '*The Projection and Measurement of cyberpower*.' In Security *Journal, Vol. 30, no.* 3.

Voo, J., Hemani, I, and Cassidy, D. 2022. *National Cyber Power Index 2022*. Cambridge, MA. Belfer Centre for Science and International Affairs.