Configuration of African Cyber Power: Three Conceptual Precepts

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

drwilhelmbernhardt@gmail.com
duvenage@live.co.za
basievs@uj.ac.za

Abstract: This paper flows from an interdisciplinary research project at the University of Johannesburg (UJ) on the design of an African-specific framework for configuring and assessing cyber power. The project advocates a nuanced and contextual approach to analysing, evaluating, understanding and enhancing cyber power in the African context, addressing the continent's unique challenges and leveraging cyber capacities for a triad of developmental, defensive, and offensive purposes. It is specifically contended that the imperative of a developmental component of cyber power distinguishes African states from the cyber power configurations of developed nations. At this very early stage of the project, the emphasis is on conceptualising theoretical constructs that can direct the design of the African cyber power triad. This paper forms part of the said theoretical quest and addresses the following problem statement: what are some primary precepts for designing an African cyber power triad? We identify and tentatively describe three precepts, namely: 1) the intentional relation between power and policy in the configuration of cyber power; 2) the centrality of national interests and security in cyber power; and 3) the imperative of optimising cyber power through the levering of asymmetric and interlocking advantages. The paper is categorically qualified as exploratory in nature and does not purport to comprehensively describe the three precepts. Instead we only advance some contours towards the academic discourse. The veracity and detailing of the proposed precepts are thus part of the ongoing research agenda.

Keywords: Cyberpower, Offensive power, Defensive power, Developmental power, National power, Africa

1. Introduction

The academic discourse on cyber power predominantly focuses on its offensive and defensive applications, the hierarchical ranking of states, and the dominance of the United States (US) military doctrine, alongside the global aspiration of developed nations. In such comparative assessments, developing states, particularly in Africa, often perform poorly and are frequently overlooked. This is despite the fact that the pursuit of cyber power is as pertinent to the national power framework of African states as it is to developed nations (Duvenage *et al*, 2023). These US-centric perspectives on cyber power are not easily transferable to other contexts and, in fact, limit the understanding of power in these environments (Cavelty, 2018). Simply put, what works for a superpower in terms of national and cyber power will likely not serve as a practical blueprint for an African country. There is thus a need for a context-dependent understanding of state power in general, and cyber power in particular. African countries' strategic national objectives may differ substantially from those of their developed counterparts, and for example typically encompass a substantial domestic, intrastate dimension, are less characterised by global ambitions and interstate rivalry, and are generally oriented towards strategic development goals.

This paper argues that Africa's unique national contexts necessitate a different conceptualisation of cyber power—one that incorporates the element of development alongside, and overlapping with, traditional notions of offensive and defensive cyber power. It proposes that African cyber power should be approached from a configurative perspective, the aim of which is to determine whether a state's cyber power profile and posture are properly aligned and optimally configured to address its unique context, derived from its national security and national interest objectives. The paper proposes and describes three essential, interrelated precepts for such an approach to the configuration of an African state's cyber power, namely:

- Acknowledging the relevance of the intentional relationship between power and policy in the configuration of an African state's cyber power;
- Aligning the state's cyber power with its national interests and security concepts; and
- Recognising the specific requirement of pursuing asymmetric, interlocking, and force-multiplying advantages through cyber power configurations in the African context.

As will be indicated, these precepts not only guide cyber power configuration, but are also normative in nature, in that they simultaneously serve as high-level 'yardsticks' for assessing a state's optimal yielding of cyber power. In conclusion, the paper brings the proposed precepts together in the form of a set of indicator-based conditional statements which, dependent on actual further empirical verification, can be employed to arrive at a more nuanced, context-appropriate analysis of the different configurations of cyber power in African states.

2. Acknowledging the Relevance of the Intentional Relationship Between Power and Policy in the Configuration of an African State's Cyber Power

National power, also referred to as a state's 'national strength' or 'national capability', encompasses a country's overall ability and resources to influence and achieve its objectives, be it on the global stage, in the domestic sphere or both. A state's power is multidimensional and uniquely configured from several components (Heywood, 2022). The elements of national power are well-documented and among others include a state's military forces, economic strength, technological advancement, natural resource endowment, geopolitical advantages, and human capital, as reflected in the quality of education and healthcare available to its population, and, for present purposes, its capacity regarding the use of cyber power. In this context, the ability to control and use information has long been recognised as a primary source of power for both state and non-state actors. Cyberspace, with its emphasis on the optimisation of digitised information and related technologies, is therefore a highly empowering capacity, which exponentially increases opportunities for state and non-state actors to wield information and other resources related to cyberspace to achieve specific ends inside and outside of cyberspace (Cavelty, 2018).

The notion of a state 'having' or 'wielding' power generally connotes a particular competence, ability, or capacity to influence the behaviour of others—be it other states or domestic role players—in a manner not of their choosing (Heywood, 2022). In this respect, attention should be given to the 'intentionality' of power - it is deliberately and purposefully created to enable the state to achieve its policy objectives (Lindvall and Teorell, 2016). There are always intended outcomes linked to the application of a state's power. National power, including cyber power, is therefore not pursued for its own sake. Instead, it is purposefully created through a deliberate investment of resources to facilitate the attainment of predetermined national policy outcomes. Lindvall and Teorell (2016) identify three distinct types of power-related resources: 1) state income (revenue); 2) human capital (the quality of state administration/skills); and 3) the availability of and access to information that enables the state to be aware of developments inside and outside its territory that may require policy interventions. The configuration of the power-related resources required to achieve national objectives will differ from state to state, depending on their respective unique situations, dynamics, intentions, and related policy objectives. In the view of the authors, the afore-mentioned views on the intentional underpinnings of power point towards the presence of a power 'value-chain', which is relevant to analysing a state's national power configuration in general, and for present purposes, also its cyber power. This 'value chain' comprises the following links:

Situational Awareness → Intended Outcome → Policy Instrument → Power Creation (resource investment) → Actual Outcome.

For the purpose of analysing and assessing an African state's cyber power configuration, the aforementioned value-chain suggests at least five normative diagnostic lines of enquiry for eventual empirical confirmation. The cyber power value, with its five diagnostic lines of enquiry (as adapted from Lindvall and Teorell, 2016) is summarised is Table 1 below:

Table 1: The cyber power value-chain

1.	**Situational Awareness:** Is there a **consciousness** or **recognition** in the state about a situational challenge, threat, problem or desired outcome that will require policy to be formulated, and an investment to be made in some type of cyber power as the means to execute the policy?
2.	**Intended Outcome/s:** What are the desired results expected or foreseen to be achieved following the application of cyber power in response to the identified situational challenge? More specifically, in what way is it foreseen that the use of cyber power will have an asymmetrical, force multiplication and/or resource optimisation impact on the desired outcome?
2.	**Policy instrument/s:** What formal 'plans' or courses of action do the state have to achieve its intended outcomes through the application of cyber power? In what way is the intended investment in cyber power conceptualised to have an asymmetrical, force multiplication and/or resource optimisation impact on the desired outcome?
3.	**Power creation:** In what **particular form or type of cyber power does the state invest** in order to implement its policies, and thus achieve its desired outcomes? What form does such an investment take, with specific reference to the allocation of revenue, skills, and/or information resources? Is the actual investment commensurate to the desired outcomes?

5.	**Actual outcome/s:** What are the actual results of policy execution or, put differently, the state's return on its cyber power investment? How did the investment in cyber power change the original situational challenge, problem or desired outcome, and how did change the state's situational awareness? Did the policy and concomitant investment in cyber power actually achieve an asymmetrical, force multiplication and/or resource optimisation impact on the desired outcome?

3. Aligning the State's Cyber Power With its National Interests and Security Concepts

As previously mentioned, national interests and national security concepts are central to the formulation of a state's national objectives. These, in turn, inform situational awareness, policies, and cyber power requirements, as outlined in the diagnostic value chain. National interests thus provide a clear starting point for evaluating the nature and extent of an African state's cyber power configuration. Bernhardt (2022) suggests that the national interests of any state, along with its national security concept (i.e. anything perceived to or actually posing a potentially existential or very serious threat to the state's national interests), generally encompass three overarching high-level strategic referent objects, encapsulated in Table 2 as follows:

Table 2: Referent Objects of the State (Bernhardt, 2022)

National Interest of the State	Description
The pursuit and protection of the continuity and survival of the state	This concerns the state's interests in maintaining its territorial integrity, national sovereignty, independence, national identity and self-determination
The pursuit and protection of the prosperity and well-being of the state	This relates to the state's interests concerning issues such as economic growth, employment, social welfare, law and order, food security, health services, energy sources, water resources, and overall quality of living
The pursuit, protection and projection of the essential values of the state	This relates to the founding ideas on which the state is premised, such as the pursuit of constitutional democracy, non-racism, non-discrimination, equality before the law, peaceful international co-existence etc, as well as to internationally values – for example the protection of human rights - to which the state subscribe

National interests, and therefore the accompanying threat perceptions and resulting national security concepts, differ from state to state, depending on their unique circumstances. Consequently, the overall national power configurations of states will also vary. For example, if a state perceives its survival to be threatened, it can be expected to allocate substantial military and other resources to policy instruments designed to neutralise such a threat. If the perceived enemy is assessed to possess offensive cyber capabilities, the threatened state would likely invest in developing a defensive cyber capacity to fend off potential cyber-attacks. Similarly, it may also identify the need for its own offensive cyber capabilities.

These generic interests of survival, prosperity, and values take on particular significance in the context of developing states. In such states, these interests often have a distinct domestic or internal focus. This is because the national security concept of these states has: "…taken on board the idea of human development" (Heywood, 2022). Human development emphasises the security of the individual within the state, in addition to, or even as opposed to, the international security of states. The actual development of the individual's economic security, food security, health security, environmental security, personal security, and political security (i.e., political rights and civil liberties) will therefore feature prominently on these states' national security agendas. Al-Mashat (2018) refers to such matters as national interests related to 'well-being,' or: "…the ability of the state to provide its public with social, economic, and political conditions conducive to happiness and a prosperous life…. This is seen as the basic element of national security in developing nations." Furthermore, "…there is little chance for any of the developing states to achieve a considerable degree of national security without increasing the state of well-being of its public." De Wet (2022) concurs, emphasising that the foremost priority of the governments of developing states should be: "…to determine, acknowledge, and prioritise the developmental needs of a society…. and to ensure that those needs are addressed in the most efficient, effective, and economical manner."

Developing states could therefore be expected to allocate a portion of their national power, including their national cyber power, to achieving their national development objectives. Confirming this, Dassah (2022) specifically notes the criticality of cyberspace in the context of development, remarking that: "…the information revolution has put information and communication technologies (ICTs) at the centre of all aspects of the lives of members of society, especially in educational, work, political, and social domains. In developed and some developing countries, this has changed and continues to change the face of public service provision in fundamental and unpredictable ways."

4. Recognising the specific Requirement of Pursuing Asymmetric, Interlocking, and Force-Multiplying Advantages Through Cyber Power Configurations in the African Context

A final notable precept applicable to all variations of a developing state's use of cyber power pertains to the anticipated asymmetric or force-multiplying advantages thereof. 'Power', as previously argued, is the intentional investment of resources to enable the state to achieve its national policy outcomes. However, in a developing state with limited resources, an investment in cyber power should enable it to 'do significantly more' (Heeks, 2001), delivering results that distinguish the previous condition (before cyber power) from the present condition (after cyber power). Ariyo (2024), supported by Malephane (2022), emphasises the criticality of cyberspace to Africa's development, particularly referencing the need for technological 'leapfrogging' to bridge development gaps in Africa. The concept of asymmetric advantages thus denotes benefits that extend beyond the obvious. Dassah (2022) succinctly highlights this point by reminding us that: "E-Government is primarily about government, not technology," implying that the focus must always be on the advantages brought about by the investment in cyber power, not on the technological investment itself. Cavelty (2018) specifically warns against "cyber-over-enthusiasm" and suggests that cyber power should be viewed as an 'auxiliary' type of power supporting other forms of power. For African countries, this implies that digital transformation in pursuit of development must avoid the "business-as-usual" approach (Ghanem, 2020). The precept of asymmetric benefits also applies to non-development-related applications of cyber power, such as cyber espionage and cyber diplomacy, or the establishment of cyber defences.

Although the three dimensions of cyber power—defensive, offensive, and developmental—are distinct and distinguishable, they are simultaneously interlocked and inseparable. Purposefully nurturing and expanding the symbiotic relationship between these dimensions is key to optimising the use of scarce resources in the African context and achieving asymmetric advantages. However, current literature lacks an integrated conceptual framework or index to guide the formulation of an overarching national cyber power policy and strategy for African states that effectively interlocks offensive, defensive, and developmental cyber power. Numerous indices and frameworks address cybersecurity (defensive cyber power), offensive cyber power, or both. Individually, these indices and frameworks are useful for concretising the African cyber power triad's offensive and/or defensive dimensions but offer limited insights into the developmental dimension. Collectively, however, they may provide pointers for designing the African cyber power triad. Çifci's (2022) survey of 11 prominent indices and frameworks is noted in this context. The precept of asymmetric advantages suggests that an interlocked and symbiotic relationship between the three dimensions of cyber power must be achieved to optimise cyber power in the African context. The following high-level, preliminary interlocking relationships are therefore proposed in Table 4:

Table 3: Interlocking relationships between the three dimensions of African cyber power

	Defensive Cyber Power	**Offensive Cyber Power**	**Developmental Cyber Power**
Definition	Ability to protect and recover the functionality of own cyber assets.	Ability to advance the national interest in cyber space through offensive operations such as espionage, surveillance, influencing operations, espionage and (cyber) war.	Ability to pursue developmental objectives in and through cyber space.
Interlock: Defensive and Offensive power	Offensive actions typically incorporate strong defensive elements. OPSEC (Operational Security) is, for example, a default design element of offensive cyber campaigns. Intelligence obtained defensively informs offensive actions. Similarly, intelligence offensively procured often guides aspects of the defensive cyber posture. Offensive cyber capabilities act as a deterrence and thus has a defensive function.		
Interlock: Defensive and Developmental power	Defensive power safeguards the cyber 'ecosystem' and tools used in pursuit of national developmental objectives. Defensive power depends on developmental power for the pipeline of human resources as well as technical tools and systems.		
Interlock: Offensive and Developmental power	Offensive power identifies threats, opportunities (e.g. through espionage, surveillance) and create circumstances conducive to developmental objectives (through for example influencing operations). Offensive power depends on developmental power for a pipeline of human resources as well as technical tools and systems.		

5. Towards Conditional Statements for Analysing Configurations of African Cyber Power

For purposes of further research, the authors have brought together the proposed precepts of African cyber power in the form of a set of indicator-based conditional statements which, dependent on actual empirical verification, can plausibly contribute to a more nuanced, context-appropriate analysis of the different configurations of African cyber-power. These statements are summarised below in Table 4:

Table 4: Formulating Conditional Statements, based on indicators, for analysing configurations of African cyber power

If	Then
If the national security concept of the African state contains situational awareness about the existence, or potential existence, of internal and/or external adversaries or enemies that are cyber-enabled, and thus need to be confronted either reactively or pro-actively in the cyber domain … Indicators: The state may require an investment in offensive cyber power if: The state has internal or external enemies or adversaries with established cyber capacities, whom it chooses to engage and oppose by means of pre-emptive neutralisation actions in cyber space due to a perceived threat to its national interests – including it development goals. The state requires intelligence on the intent and capacity of its enemies and/or other adversaries, which necessitates a resort to espionage. The state intends embark on espionage in cyber space in order to obtain a competitive edge in matters related to its economic prosperity, diplomatic relations or international policy objectives.	Then an intentional investment can reasonably be expected in cyber resources that will endow the state with an asymmetric offensive cyber power capacity, And - The extent or weight of the investment in such cyber power will be determined by the number of such enemies, as well as the level of sophistication assigned to their cyber capacity and adversarial intent, as well as the economic ability and political will of the state to invest the requisite resources for the creation of such power.
If the national security concept of the African state contains situational awareness about referent objects of the state that are cyber connected, and thus vulnerable to cyber-attack, subversion, sabotage, or intrusion… The state may require an investment in defensive cyber power if the following indicators are present: The state's sovereignty of decision-making is at risk from undue influencing or manipulation of its political, policy and/or electoral processes by adversaries with the assistance of cyber-based strategies. The state's internal stability is at risk from cyber-enabled terrorists, insurrectionists, or rebel activity. The state is characterised by distinct vulnerabilities in its cyber defences, which renders it susceptible to cyber-based attacks by internal or external cyber-empowered enemies or adversaries. The state experiences challenges to adequately protect its or its finances against possible or actual cyber-attacks. The state experiences challenges to adequately protect its critical infrastructure, privileged information, and/or resources against possible or actual cyber-attacks.	Then an intentional investment can reasonably be expected in cyber resources that will endow the state with an asymmetric defensive cyber power capacity, The extent or weight of the investment in such cyber power will be determined by the extent and degree of the state's cyber vulnerability; the number of past incidents indicative of cyber exploitation, the actual presence of enemies or adversaries with the intent and capacity to exploit such vulnerabilities, as well as the economic ability and political will of the state to invest the requisite resources for the creation of such power.
If the national security concept of the African state contains situational awareness about the need for, protection of or advancement of development as a referent object of security… The state may require an investment in developmental cyber power if the following indicators are present: The state is vulnerable in terms of real time, integrated access to all data relevant to its development. The state experiences challenges in respect of delivering effective and efficient governance services to all citizens. The state has a history of colonialism, poverty, and underdevelopment. The state experiences insufficient economic growth. The state's labour market reflects high levels of unemployment.	Then an intentional investment can reasonably be expected in cyber resources that will endow the state with an asymmetric developmental cyber power capacity, The extent or weight of the investment in such cyber power will be determined by the prominence, urgency, or priority that the state affords to development as a component of its national security concept, as well as the economic ability and political will of the state to invest the requisite resources for the creation of such power.

If	Then
The state is characterised by significant challenges related to the delivery of basic services in respect of human security, such as education, health, water, food, sanitation, refuse removal, social security, and electricity.	

6. Conclusion

This paper posits that a context-specific configuration of African cyber power should begin with an examination of the prompts for cyber capacity building provided by the state's national interests and security concepts. Parallel to this, there should be a mapping of African states' respective cyber power value-chains to determine the continuity of the intentional relation between prompt, power, policy, and outcome. Regarding policy outcomes, the presence of asymmetric, interlocking, and force-multiplying advantages must be assessed. It concludes with an integration of these precepts in the form of a proposed set of indicator-based conditional statements for the configuration of African cyber power. While the ultimate aim of this research is to empirically profile African states' respective cyber power configurations, it is acknowledged that the research remains predominantly normative, and much empirical groundwork is yet to be completed in order to be verified and refined. The validity and reliability of the proposed precepts of cyber power, and the accompanying conditional statements for configuring African cyber power are therefore still to be substantiated by means of future research.

References

Al-Mashat, A.M. 2018. *National Security in the Third World*. London and New York. Routledge.

Ariyo, O. 2024. *Closing the digital divide in Africa: unfolding challenges, strategies, and success stories*. In The Cable. 19 March 2024. https:/thecable.ng/closing-the-digital-divide-in Africa-unfolding-challenges-strategies-and-success-stories, Accessed 2024/06/06.

Bernhardt, W. 2022. *Strategic Intelligence in the Context of National Security*. Lecture presented at the University of Pretoria, Masters in Security Studies Course, SEC879 Strategic Intelligence and Forecasting (2022/04/25).

Dassah, M. O. 2022. *Role of technology in the functioning of the state*. In Thornhill, C., Van Dijk, G., and Ile, I. (Eds.). 2022. *Public Administration and Management in South Africa. A Developmental Perspective*. Cape Town. Oxford University Press.

Davids, I. 2014. *Development Theories: Past to presen*t. In Davids I. and Theron, F. (Eds.). 2014. *Development, the state and civil society in South Africa*. Van Schaik Publishers. Pretoria.

De Jager, N. 2021. (Ed.). *South African Politics. An Introduction*. Cape Town. Oxford University Press Southern Africa.

Dunn Cavelty, M. 2018. *Europe's cyber-power*. In European Politics and Society, 2018, Vol. 19. No 3, pp. 304 – 320.

Duvenage, P., Von Solms, S., and Bernhardt, W. 2023. *Cyber power in the African context: an exploratory analysis and proposition*. June 2023 European Conference on Cyber Warfare and Security 22(1): 177-186.

Ghanem, H. 2020. *Shooting for the moon: An agenda to bridge Africa's digital divide*. In The Brookings Institution. 7 February 2020. https:/brookings.edu/papers/shooting-for-the-moon-an-agenda-to-bridge-africas-digital-divide/. Accessed 2024/06/06.

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

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

Heeks, R. 2001. *Understanding e-governance for development*. I-Government Working series, No. 11. Precinct Centre, Manchester: Institute for Development Policy Management, University of Manchester. https://s.ssrn.com/sol3/s.cfm?abstract_id=3540058. Accessed on 30 April 2024.

Heywood, A. 2022. *Politics*. Bloomsbury Academic. London.

Kotze, J.S. 2021. *Introduction: The theory and practice of democratic development*. In De Jager, N. 2021. (Ed.). *South African Politics. An Introduction*. Cape Town. Oxford University Press Southern Africa.

Lindvall, J., and Teorell, J. (2016). State Capacity as Power: A Conceptual Framework. (STANCE Working
Series; Vol. 2016, No. 1). Department of Political Science, Lund University.

Malephane, L. 2022. *AD582: Digital Divide: Who in Africa is connected and who is not*. In Afrobarometer, 14 December 2022. https:/www.afrobarometer.org/publication/ad582-digital-divide-who-in-africa-is-connectedand-who-is-not/. Accessed 2024/06/06.

Schick, A. 2003. The performing state: reflection on an idea whose time has come but whose implementation has not. In OECD Journal on Budgeting. 3 (2): 71 – 103.

Snow, D.M. 2004. *National Security for a new era. Globalisation and geopolitics*. Pearson Longman. New York.

Swanepoel, H. 1997. Community development: putting plans into action. 3rd edition. Cape Town. Juta. As quoted in In Davids I and Theron, F. (Eds). 2014. Development, the state and civil society in South Africa. Van Schaik Publishers. Pretoria.

Thornhill, C., Van Dijk, G., and Ile, I. (Eds.). 2022. *Public Administration and Management in South Africa. A Developmental Perspective*. Cape Town. Oxford University Press.