South Africa as a Continental Cyberpower: What do Some Scorecards say?

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

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

Abstract: South Africa's role as a continental leader, and its ability to address domestic challenges, both now and to an increasing degree in the future, will depend on its ability to optimise cyberpower. While there are several frameworks and indices designed to assess cyberpower, or aspects thereof, none of these are specifically designed to factor in the developmental imperative of African countries and the Global South. This paper forms part of a research project at the University of Johannesburg aimed at the design of an Africa-specific model for configuring and evaluating cyberpower. The African Cyberpower Triad is a three-dimensional model that elevates the developmental imperative to be on an equitable footing with offensive and defensive cyberpower. At this early stage of our research, cyberpower-related assessment indices and frameworks are being evaluated for possible use in the design of the African Cyberpower Triad. This paper derives from this appraisal and has as its central research questions: 'What are some of the cyberpower-related instruments that can be utilised as 'scorecards' to measure and/or assess aspects of South African cyberpower', and 'what do they say about South Africa's status as a cyberpower in the African context'? The paper identifies and applies scorecards relevant to all three dimensions of cyberpower. The scorecards indicate that, within the continental context, South Africa is a major cyberpower with significant but, in various respects, unrealised potential. Harnessing this potential will require strong political will and the decisive implementation of a well-rounded national cyber strategy that synthesises the offensive, defensive and developmental dimensions. Regarding offensive cyberpower, scorecards suggest that South Africa is a major player on the continent, but not the leading force at present. In terms of defensive cyberpower, South Africa scores well above the international average, yet it does not rank as a continental role model. However, South Africa ranks highly as a leading developmental cyberpower—though also in this instance its capacity remains far from fully realised. This paper presents a preliminary and exploratory evaluation, to be followed by a comprehensive assessment of South Africa's status as a continental cyberpower, based on the model currently under development.

Keywords: Cyberpower, Cyber power, Africa, South Africa, Global South, Cybersecurity, Development

1. Introduction

South Africa is a continental leader in various respects. According to the International Monetary Fund (IMF) South Africa is not only Africa's most industrialised economy, but also its largest. It is projected that South Africa will maintain this position until at least 2027 (Michela 2024). When quantified more precisely, South Africa's Gross Domestic Product (GDP) of $373 billion in 2024, tops that of Egypt ($347bn), Algeria ($266bn), Nigeria ($252bn) and Ethiopia ($205bn) (Micheal 2024). Despite systemic issues and challenges, South Africa's military is still rated as the third most powerful on the continent and behind only that of Egypt and Algeria (Global Firepower 2024). A nation-state's standing and national power are of course not only shaped by 'hard' measurables, but consideration must also be given to intangible elements such as political stability, diplomatic influence, and cultural impact. In these respects South Africa is undoubtedly a continental leader. Apart from its prominent role in Africa, South Africa is widely seen as a "pivotal middle-ground state" having substantial leverage in the Global South (Devanny & Buchan 2024; van Nieuwkerk 2024). With respect to overall national power, the World Power Index ranks South Africa as the leading country in Africa followed by Egypt, Algeria, Morocco and Nigeria (Ruvalcaba 2023). Despite this standing, South Africa, like many of its African peers, is daunted by domestic political and socio-economic developmental challenges, such as high unemployment, inequality, and crime, all of which impede its economic growth and social cohesion.

South Africa's ability to address these domestic challenges and exert power regionally and continentally, will increasingly depend on optimising its use and configuration of cyberpower. Assessing South Africa as a cyberpower within the context of it being a developing African country would be a useful start. Phrased differently, South Africa's cyberpower needs to be 'measured up' in the African context to inform an optimal configuration. While there are numerous frameworks used to assess cyberpower, or aspects thereof (notably cybersecurity), none of these are specifically designed to account for the developmental challenges faced in the African milieu. This paper forms part of research at the University of Johannesburg aimed at the design of an Africa-specific model for configuring and assessing cyberpower. This model, referred to in short as the African

Cyberpower Triad, is a three-dimensional construct elevating the developmental imperative to an equitable footing with offensive and defensive cyberpower.

At this initial stage, the research project's focus is twofold. Firstly, to design the theoretical constructs that will guide the model's design, and secondly, to examine existing cyberpower-related assessment indices and frameworks (hereafter collectively referred to as instruments or 'scorecards'). This paper forms part of the second research focus, and has as its central research questions: What are some of the cyberpower-related instruments that can be utilised as 'scorecards' to measure and/or assess aspects of South Africa's cyberpower? What do they say about South Africa's status as a cyberpower in the African context?

To address these research questions, the rest of the paper is structured as follows:

- Section 2 explains the African Cyberpower Triad as the premise for the selection of instruments used in assessing South Africa's cyberpower.
- Utilising selected scorecards, Sections 3 to 5 assess the three dimensions of South African cyberpower, namely offensive cyberpower (Section 3), defensive cyberpower (Section 4) and developmental cyberpower (Section 5).
- Based on the assessment of these dimensions, Section 6 summarises the findings and concludes the paper by noting that a holistic assessment comprises an area of ongoing research.

Within the confines of a conference paper, we are highly selective in our approach and do not in any way purport to offer a comprehensive assessment of all instruments. Neither do we contend that the composition of instruments, methodologies and outcomes are incontestable. The use of these instruments in this paper should be seen for what it is: exploratory and tentative research that will ultimately inform the design of a cyberpower model. It is our aim that this model be useful, not only to South Africa, but African countries generally.

2. The African Cyberpower Triad as Premise for Scorecard Selection

This section consists of two subsections. Subsection 2.1 explains the African Cyberpower Triad and recapitulate previous research in this regard. Based on this conceptual premise, Section 2.2 examines the implications for our scorecard selection.

2.1 An Outline of the African Cyberpower Triad

Cyberpower can broadly be defined as that component of national power directed towards safeguarding and advancing national interest through and within cyberspace (United Kingdom 2022; BAE 2022; Devanny 2021; Voo, Hemani and Cassidy 2022). Although few would contest this definition, the academic discourse in the Global North has until as recently as a decade ago been predominated by cyberpower's offensive dimension which emphasises force and coercion within the realm of interstate conflict (Cavelty 2018). Cybersecurity was deemed relevant to, but not at the centre of, the discourse on cyberpower. Presently there is consensus that 'cyberpower' has a fundamental second dimension, namely defensive cyberpower which has a "strong cyber-security element" and includes resilience (Cavelty 2018). Defensive cyberpower is now axiomatically positioned as inextricably linked to offensive power. Cyberpower remains a dynamic and fast-evolving concept. Presently the cyber strategies of some of the developed, major powers such as the United Kingdom (2022), link cyberpower more explicitly to socio-economic objectives. Within Africa, and the rest of the developing world, these socio-economic objectives are, first and foremost, developmental in nature. For this reason, the development imperative should be at the centre of cyberpower in Africa specifically, and the Global South generally, both academically and in practice.

As referred to in Section 1, this paper is premised on earlier research (Duvenage, Bernhardt and von Solms 2023) and concurrent work (Bernhardt, Duvenage and von Solms 2025) which contend that the configuration of cyberpower in the African context should be expanded to a three-dimensional construct elevating the developmental focus. The Cyberpower Triad holds cyberpower as being constituted by offensive, defensive and developmental dimensions of equitable weight and importance. For context and clarity, the Cyberpower Triad's dimensions, as expounded in our other research, are briefly recapitulated (Duvenage, Bernhardt and von Solms, 2023; Bernhardt, Duvenage and von Solms 2025):

- Offensive cyberpower refers to the advancement of national interest in cyberspace through a combination of force, coercion, aggressive influence, and intrusion. It includes actions such as espionage, surveillance, influence operations, and cyber warfare.

- Defensive cyberpower focuses on the protection of a nation's systems and networks. It involves measures to prevent, detect, and respond to cyber threats, as well as building the resilience of cyber-related assets.
- Developmental cyberpower signifies the ability to achieve developmental goals in cyberspace, working synergistically with defensive and offensive dimensions. It entails a country's collective cyber capacity that is relevant, or potentially relevant, to its national developmental priorities.

Building on this premise of a three-dimensional cyberpower model, the next section outlines our approach to the selection of scorecards.

2.2 Approach to the South African Cyberpower Assessment and Scorecard Selection

The concepts above guided our selection of scorecards to be used in assessing South Africa's cyberpower within the African context. Given our cyberpower postulation (in subsection 2.1), such an assessment has as its first requirement an equitably apportioned capacity to measure offensive, defensive and developmental cyberpower. A second requirement is that the scorecards should preferably assess South Africa as it relates to other African countries. As will be elaborated on in Section 3, the two existing cyberpower indices do not have development as a primary focus. As Section 3 will further show, only one index assesses South Africa and that in comparison to only one other African country. Consequently, it was necessary to expand our selection of scorecards, adopting a broader approach that also considers numerous instruments globally assessing cyberpower-relevant aspects, such as cybersecurity, e-governance, ICT development and the leveraging of cyber capacity for development purposes. From these instruments, we selected scorecards that could serve as indicators of South Africa's developmental and defensive cyberpower. This selection and outcome are presented in Section 4 (defensive cyberpower) and Section 5 (developmental cyberpower). The more complex challenge of assessing South Africa's offensive cyberpower is addressed in the next section.

3. South Africa's Offensive Cyberpower

Of the three dimensions, the assessment of a nation-state's offensive cyberpower is the most difficult to explore academically and assess comparatively (IISS 2023). The Belfer Centre rightly states "… components that contribute to a state's cyber power are sensitive and therefore classified. Due to the sensitivities of … particularly destructive, defensive and espionage capabilities … states may deliberately be shielding their intent and capabilities." (Voo, Hemani and Cassidy 2022). Therefore, "an absence of evidence" for the existence of offensive cyber capabilities "does not equate to evidence of their absence" (IISS 2023).

As far as could be ascertained from our literature study, there are only two current instruments with the stated aim of assessing cyberpower – those being the 'National Cyber Power Index' (NCPI) published by the Belfer Centre for Science and International Affairs (Voo, Hemani and Cassidy 2022), and the International Institute for Strategic Studies' (IISS 2021, 2023) 'Cyber Capabilities and National Power' (CCNP). A concise comparison of the instruments is provided in **Table 1** (on the next page).

While these indices include aspects of defensive cyberpower, they were employed for the purposes of this paper, strictly for an appraisal of South Africa's offensive cyberpower. Given the complexity of measuring offensive cyber capacities, both indices strongly rely on qualitative judgments. It must be emphasised that both indices, unlike cybersecurity instruments discussed in Section 4, assesses a limited number of selected nation-states.

Table 1: Comparison of the cyberpower assessment instruments

	National Cyber Power Index (NCPI)	**Cyber Capabilities and National Power Assessment (CCNP)**
	Belfer Center	International Institute for Strategic Studies (IISS)
Methodology	Quantitative and qualitative	Qualitative
Scope	30 countries	25 countries

	National Cyber Power Index (NCPI)	**Cyber Capabilities and National Power Assessment (CCNP)**
	Belfer Center	International Institute for Strategic Studies (IISS)
Assessment pillars	Surveillance and monitoring of domestic groups Strengthening and enhancing national cyber defences Controlling and manipulating the information environment Foreign Intelligence collection for national security Growing national cyber and commercial technology competence Destroying or disabling an adversary'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

Sources: (Voo, Hemani and Cassidy 2022; IISS 2021, 2023)

Generally African countries lag in both cyberpower indices. The NCPI's ranking of the top cyber powers in descending order are as follows: United States, China, Russia, United Kingdom, Australia, Netherlands, Vietnam, South Korea, France, Iran, Germany, Ukraine, Canada, North Korea , Spain, Japan, Singapore, New Zealand, Israel, Sweden, Saudi Arabia, Switzerland, Türkiye, Egypt, Estonia, India, Italy, Malaysia, Lithuania and Brazil (Voo, Hemani and Cassidy, 2022). The only African country listed, namely Egypt, is ranked in 24th place, which means that it does outpace other countries with their significant and proven offensive cyber capacities such as Estonia, India and Italy (Voo, Hemani and Cassidy 2022). South Africa does not feature in the NCPI, but the inclusion of Egypt and Brazil provided comparative context for evaluating South Africa later in this section.

The CCNP (IISS 2023) does not assess Egypt, but the 25 countries it evaluates include South Africa, Nigeria and Brazil (with the latter also ranked by the NCPI). The CCNP does not quantitatively rank each state but instead employs a clustering into three tiers. In a tabulated format the outcome of the assessment is as follows (IISS 2021, 2023):

Table 2: Cyber Capabilities and National Power Assessment

Classification	**Countries**
Tier 1: World-leading strengths in all aspects.	United States
Tier 2: World-leading strengths in some respects.	United Kingdom, France, Israel, Australia, Canada, China, Russia, Germany, Netherlands
Tier 3: Strengths or potential strengths in some categories but substantial weaknesses in others.	India, Indonesia, Iran, Japan, Malaysia, North Korea, Vietnam, Brazil, Estonia, Nigeria, Saudi Arabia, Singapore, South Africa, Türkiye, United Arab Emirates (UAE)

Sources: IISS 2021, 2023

Although the CCNP refrains from quantitively ranking countries within each tier, its qualitative country assessments provide a basis for a comparison of countries' relative power. In respect of Tier Three, the CCNP states: "Brazil, Nigeria and South Africa face the challenges of developing countries in building up their cyber capabilities …. That said, Brazil appears to be in a stronger position than the other two" (IISS 2023). As previously stated, the NCPI posits Egypt as outpacing Brazil in cyberpower. Although the CCNP and NCPI differ in methodology, it can thus be asserted that Egypt outweighs Nigeria and South Africa in offensive cyberpower.

The CCNP assesses Nigeria and South Africa as possessing modest offensive cyberpower that is overwhelmingly domestically focussed (IISS 2023). A comparative analysis of the CCNP's country assessments suggests Nigeria

as presently having a slight edge over South Africa in the building of cyber-intelligence, cybersurveillance and cyberwarfare capabilities (IISS 2023). The IISS's (2023) appraisal of specific aspects of South Africa's offensive cyberpower is summarised in Table 3.

Table 3: IISS – Assessing aspects of South Africa's offensive cyberpower

Offensive strategy	Lacks an overarching offensive cyber strategy. Strategy for military use of cyber is nascent. Institutional mechanisms and capacity in offensive cyberpower are deficient and hamstrung.
Cyber command and control	Has yet to achieve full operational status.
Cybersurveillance	Cybersurveillance platforms exist for law enforcement and possible domestic surveillance.
Cyber-intelligence, espionage and cyber counterintelligence.	Limited cyber-intelligence capabilities are focused on domestic/African interests. Has the will, but limited ability, to "track" major cyber powers. Highly reliant on foreign technology.
Offensive cyberoperations	The military may use offensive cyber capabilities to pursue information superiority, but "has yet to develop significant offensive [military] cyber capabilities." Doctrines on cyber operations are lacking.

Source: Compiled from narrative in IISS (2023)

The IISS (2023) notes South Africa for its robust ICT infrastructure, vibrant start-up scene, advanced digital economy, with strong tertiary institutions, as well as advances in Artificial Intelligence (AI). While South Africa "ranks highly in Africa in most measures of digital development" (IISS 2023), it has yet to leverage this advantage in the form of a homegrown offensive capacity. As a result, South Africa potentially possesses some of the most sophisticated cyber capabilities in Africa (Devanny and Buchan 2024) but is presently not the leading offensive cyberpower in Africa. On a global scale, South Africa's offensive cyber capabilities are very modest and in the pilot stages of development (IISS 2023, Devanny and Buchan 2024). An interpretive analysis of the scorecards (IISS 2023, Devanny and Buchan 2024, Voo, Hemani and Cassidy 2022) and other research we conducted points to South Africa's significantly restricted offensive cyberpower being the result of an under-prioritised state-led effort that is deficient in strategy, and in translating intent or will into sustained concrete deliverables.

4. South Africa's Defensive Cyberpower

Defensive power, as defined in Section 2, has cybersecurity and resilience as two of its principal components. It is important to note that defensive cyberpower is broader than only cybersecurity and resilience in that it is interconnected with, for example, military defence. This is reflected in the assessment pillars of both the CCNP (IISS 2023) and NCPI (Voo, Hemani and Cassidy 2022) as depicted in Table 1. Although the CCNP qualitatively ranks defensive cyberpower in this broader context, the index, as mentioned in Section 3, is extremely limited in the scope of the African countries it covers. For the purposes of this paper, cybersecurity assessment instruments (also measuring resilience aspects) with a global coverage were thus examined as possible scorecards for South Africa's defensive cyberpower. Such indices admittedly do not cover all facets of defensive cyberpower, but can nevertheless serve as a useful, if only partial, indicator.

Çifici (2022) identifies three cybersecurity indices with global coverage, namely the ITU Global Cybersecurity Index (GCI), the National Cybersecurity Index (NSI) of the e-Governance Academy of Estonia (2023) and the University of Oxford's Cybersecurity Capacity Centre's (2024) Cybersecurity Capacity Maturity Model for Nations (CMM). Both the GCI and CMM are well established and have been applied and refined for several years. The CMM, however, has not conducted a fully-fledged evaluation of South Africa and the "desktop assessment" that was carried out is not publicly available (C3SA 2021). As a result, the CMM had to be excluded as a scorecard. We are still assessing the possible use of the NSI for the African model's design looking especially at methodological aspects. Of the three cybersecurity ndices with global coverage, both the NSI and CMM were thus ruled out at this stage for the reasons indicated, and the ITU's GCI 2024 edition was selected as an indicator of South Africa's defensive cyberpower in the African context.

The GCI quantitively measures 194 countries' commitment to cybersecurity through five pillars: legal measures, technical measures, organisational structures, capacity building, cooperation, and confidence-building measures (ITU 2024). A maximum index point of 100 is assigned and country performance classed from Tier 1 'Role-

Modelling' to Tier 5 'Building'. With an index point of 86,25, the GCI (2024) positions South Africa well above the global and African average. Considering South Africa's national power and continental standing generally, a comparison with some of its African peers as provided in Table 4, however, raises concern:

Table 4: Global Cybersecurity Index (GCI) – African top 14 countries

Africa rank	Country	Score	Tier
1	Mauritius	100	Tier 1 Role modelling
1	Egypt	100	
3	Kenya	99.49	
4	Ghana	99.27	
5	Tanzania	99.26	
6	Rwanda	98.08	
7	Morocco	97.50	
8	Zambia	92,59	Tier 2 Advancing
9	Benin	91,54	
10	Togo	88,80	
11	South Africa	86,25	
12	Uganda	83.02	Tier 3 Establishing
13	Nigeria	82.58	
14	Tunisia	82	

Source: ITU 2024

Given South Africa's political prominence in cyber-related matters in Africa, the size of its industrialised economy and its advanced ICT infrastructure, its ranking in 11th position and as a low Tier 2 country in the GCI, fall short of expectations. It would have been expected that South Africa's high cyber-threat profile (with regard to intensifying and an expanding range of cyber-based threats) would have prompted intervention to ensure the prioritised allocation of national power resources to cyber defences. In this regard it is worth noting, that the GCI ascribes "a significant portion" of each country's performance in the index to "to the coordinated measures and interventions by its national government to improve national cybersecurity capabilities" (ITU 2024). South Africa is clearly a case in point, with political pronouncements on cybersecurity prioritisation not consistently mirrored by concrete action and the commitment of resources. The GCI shows South Africa as underperforming in the assessment pillars of "Organisational Measures" and "Capacity Development." More concretely, underperformance in these areas manifest as low investment in cyber education, shortage of cyber-security professionals, lethargic implementation of cyber policy and legislation, as well as deficient institutional cooperation (IISS 2024). The GCI further notes the importance of public-private partnerships (PPPs) in bolstering cybersecurity (ITU 2024). This is particularly relevant to South Africa given its significant private sector cyber capacity. In all, improving South Africa's defensive cyberpower will depend on strong political will and support of a state-led, cooperative, cybersecurity endeavour. At the time of writing there is a widening gap between South Africa's intent and the actual conversion of will into action.

This section reviewed the GCI as an indicator of South Africa's defensive cyberpower. In the next section, South Africa's developmental cyberpower is examined by employing two other global indices.

5. South Africa's Developmental Cyberpower

In Section 2 we observed that developmental cyberpower pertains to a nation-state's collective cyber capacity as relevant to its national developmental priorities. From the perspective that this capacity has human, institutional, technical and infrastructural facets; we surveyed indices with the aim of assessing two critical

aspects of developmental cyberpower, namely effective e-governance and the capacity of a state to leverage information and communication technologies (ICTs) for development. The two indices selected for scorecards of South Africa's developmental cyberpower are both highly regarded and have been in operation for more than twenty years, namely the E-Government Development Index (EGDI) and the Network Readiness Index (NRI). The EGDI measures the capacity and effectiveness of digital governance, online services, and assesses human capital, while the NRI evaluates readiness for the digital economy by gauging aspects such as ICT access, usage, and impact. Used in combination, these indices evaluate aspects highly pertinent to assessing the aforementioned two critical dimensions of developmental cyberpower, namely effective e-governance and the capacity of a state and society to leverage ICTs for development. On this basis, we deemed the EGDI and NRI as the most suitable at this stage of the African cyberpower model's development.

The United Nations' EGDI debuted in 2001 as an instrument to appraise the e-government development of countries at a national level (UN 2024). The 2024 EGDI report surveyed 193 participating countries (UN 2024). It is a composite measure that incorporate three UN indices, namely the Telecommunications Infrastructure Index (TIE), the Human Capital Index (HCI), and the Online Service Index (OSI). Its 2024 ranking of the top 10 African countries is as follows:

Table 5: E-Government development index (EGDI) 2024 - African top ten countries

Africa Rank	Country	EGDI Score	Rating Class
1	South Africa	0.8616	Very High
2	Mauritius	0.7506	Very High
3	Tunisia	0.6935	High
4	Seychelles	0.6773	High
5	Morocco	0.6841	High
6	Egypt	0.6699	High
7	Ghana	0.6317	High
8	Kenya	0.6314	High
9	Cabo Verde	0.6238	High
10	Botswana	0.6118	High

Source**:** UN 2024

The EGDI places South Africa, alongside Mauritius, as the first African countries to achieve a 'very high' EGDI ranking (Chacha and Barclay 2024). An analysis of the EGDI survey, and its composite indices, shows South Africa as strong in telecommunications and digital infrastructure, functional institutional frameworks and policies, as well as having made substantial progress in providing government services through digital platforms in some areas. Despite leading in e-governance generally, South Africa faces considerable challenges in addressing disparities in the provision of, and access to, digital services; digital literacy and skills development. Further, inequalities exist in empowering rural areas and local government. The EGDI shows interoperability between different government systems and services as a further challenge.

The Network Readiness Index (NRI), first launched in 2002 by the World Economic Forum, is currently published by the US-based Portulans Institute and the Saïd Business School at the University of Oxford (Portulans Institute 2024) The index aims to gauge nation-states' capacity to utilise information and communication technologies (ICTs) for socio-economic development. The 2024 edition assessed 133 nation-states, of which the top ten in Africa (given in descending order) are:

Table 6: Network Readiness Index (NRI)

Africa rank	Country	World rank
1	Mauritius	60
2	Seychelles	71
3	South Africa	72
4	Kenya	73
5	Morocco	76
6	Egypt	85
7	Ghana	87
8	Rwanda	91
9	Côte d'Ivoire	92
10	Tunisia	96

Like the EGDI, the NRI points to South Africa as a continental leader in developmental cyberpower. South Africa shows strength in technological Infrastructure, legislation, infrastructure and the adoption by business of technology (Portulans Institute 2024). This is reflected in the high ratings for the digitalisation of businesses, e-commerce legislation, cloud computing, investment in telecommunication services, and software spending (Blue Sky 2024). Conversely, government investment in research and development is low and challenges exist in the area of ICT skills development, as well as broad-based upliftment and education. Above all, it should be noted that South Africa ranks very low in the 'impact' pillar, highlighting the necessity to translate network readiness into broad-based tangible societal benefits, thus alleviating inequality (Portulans Institute 2024).

South Africa clearly faces significant challenges in harnessing developmental cyberpower to reduce inequality, enhance governance, and drive economic growth. Much like its defensive and offensive cyber capabilities, the country does not yet succeed in translating strategic intent into coordinated, sustained action. South Africa's *National Development Plan 2030* (adopted in 2012), for example, recognises the crucial role of ICT and calls for a "single cohesive strategy to ensure the diffusion of ICTs across all sectors." However, a unified developmental strategy remains lacking. While some government departments have made notable progress in leveraging cyber capabilities for development, others continue to lag. Furthermore, weaknesses in state-led cybersecurity efforts contribute to high levels of cybercrime, compounding these challenges. Our ongoing research focuses on optimising South Africa's developmental cyberpower to address these pressing issues.

6. Conclusion

This paper is based on the key premise that an Africa-specific model for configuring and assessing cyberpower is a three-dimensional construct comprising offensive, defensive and developmental cyberpower. In order to inform the development of this model, we considered cyberpower-related instruments that are useful for assessing South Africa's cyberpower in the African context. We noted that these scorecards are not only possible to dispute, but also that they measure only a few facets of a much wider and more complex construct. With this qualification, the key scorecard findings are as follows:

- Since countries typically shield parts of their offensive cyber capabilities and intent, this dimension is difficult to credibly assess. Nevertheless, going on information in the public domain, South Africa seems to have limited offensive capabilities and these that are mainly focused on domestic and African interests. While it has great offensive potential, South Africa, at present, appears to be trailing Egypt, and to a lesser degree Nigeria.
- Within Africa, South Africa scores highly in numerous measures of digital development that includes the critical aspects of e-governance and network readiness. South Africa ranks as continental leader in developmental cyberpower, with the primary challenge being leveraging this power in a coordinated, sustained manner to reduce inequality.

- South Africa's digital advancement, economic strength and political stature create the expectation that it would be a leading continental player in defensive cyberpower. While the ITU (2024) scores South Africa above the continental median, South Africa is however not rated as one of the seven 'role modelling' African countries. In short, South African developmental cyberpower is above average in score, but far below expectation.

Scorecards are useful, but as has been emphasised repeatedly, insufficient. Nonetheless, an interpretive analysis of even the few scorecards used in this paper suggests the translation of intent and South Africa's rich potential into concrete deliverables as a primary challenge. Optimising South Africa's cyberpower clearly will depend on strong political will and the design and decisive implementation of a cohesive, national cyber strategy that synthesises the offensive, defensive and developmental dimensions.

We emphasise our assertions on South Africa's cyberpower as largely tentative inferences. A credible assessment of South Africa's cyberpower would require an in-depth analysis of each dimension and, above all, an integrated appraisal that places cyberpower within the context of South Africa's national power and the challenges faced as a developing Africa country. The cyberpower model currently under development is precisely intended to serve as a conceptual basis for such an appraisal of South Africa and other African countries. When employed as part of such a model, the scorecards examined in this paper can indeed serve as useful instruments for assessing and configuring aspects of cyberpower.

References

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

Bernhardt, W., Duvenage. P. and von Solms. (2025). *Configuration of African Cyber Power: Three Conceptual Precepts*. Submitted to the 24th European Conference on Cyber Warfare and Security (ECCWS), Kaiserslautern, Germany.

Blue Sky. Education. (2024) *30 African nations feature in global Network Readiness Index 2024*. Available at https://pressreleases.responsesource.com/news/105962/african-nations-feature-in-global-network-readiness-index-mauritius/.

Chacha, L and Barclay, C. (2024) *Mapping Africa's Cybersecurity Development - Insights from the Global Cybersecurity Index 2024*. Available at (PDF) Mapping Africa's Cybersecurity Development - Insights from the Global Cybersecurity Index 2024

Cybersecurity Capacity Centre for Southern Africa (C3SA) (2021) Southern *African Development Community Cybersecurity Maturity Report 2021*. Available at http://hdl.handle.net/11427/36211t

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

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

Devanny, J., & Buchan, R. (2024) *South Africa's Cyber Strategy Under Ramaphosa: Limited Progress, Low Priority*. Carnegie Endowment for International Peace. https://carnegieendowment.org/2024/01/12/south-africa-s-cyber-strategy-under-ramaphosa-limited-progress-low-priority-pub-9137

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

e-Governance Academy of Estonia. (2023) National *Cybersecurity Index*. – archived 2016-2023. Available at https://ncsi.ega.ee/ncsi-index/?archive=1

Global Firepower. (2024). *African Military Strengths*. Available at https://www.globalfirepower.com/countries-listing-africa.php.

International Institute for Strategic Studies (IISSS). (2021) *Cyber Capabilities and National Power: Net Assessment, Volume 1.* Available at https://web-opti-prod.iiss.org/research-paper/2021/06/cyber-capabilities-national-power/

International Institute for Strategic Studies (IISSS). (2023) *Cyber Capabilities and National Power: Net Assessment, Volume 2*. Available at https://www.iiss.org/research-paper/2023/09/cyber-capabilities-national-power-volume-2/

International Telecommunication Union (ITU). (2024) *Global Cybersecurity Index 2024.* Available at https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Global-Cybersecurity-Index.aspx.

Michael, C. (2024) Africa's GDP giants: Top 10 largest economies of 2024 – IMF. *Business Day*. Available at https://businessday.ng/news/article/africas-gdp-giants-top-10-largest-economies-of-2024-imf/

Oxford Global Cybersecurity Centre. (2024) *Cybersecurity Capacity Maturity Model for Nations (CMM) – Reviews around the World: 2024 . Available at https://gcscc.ox.ac.uk/cmm-reviews*

South Africa (Republic of). National Planning Commission. (2012). *National Development Plan 2030: Our future - make it work*. Available at https://www.gov.za/documents/national-development-plan-2030.

Portulans Institute and Saïd Business School. (2024) *Network Readiness Index 2024*. Available at https://download.networkreadinessindex.org/reports/data/2024/nri-2024.pdf

Ruvalcaba, M. D. (2024) World *Power Index Database*. Available at https://www.worldpowerindex.com/wpi-database/

United Kingdom 2022. Nation Cyber Strategy 2022. Available at https://www.gov.uk/government/publications/national-cyber-strategy-2022.

United Nations (UN) Department of Economic and Social Affairs. (2024). *United Nations E-Government Survey 2024: Accelerating Digital Transformation for Sustainable Development with the Addendum on Artificial Intelligence*. New York: United Nations. https://digitallibrary.un.org/record/4061269.

van Nieuwkerk, A. (2024) South Africa's Foreign Policy Constraints and Opportunities in the Changing World Order (2020-2024), *Journal of African Foreign Affairs*, Vol 11, Nr 2: 103-121

Voo, J., Hemani, I, and Cassidy, D. (2022) *National Cyber Power Index 2022*. Cambridge, MA. Belfer Centre for Science and International Affairs. Network Readiness Index (NRI). Available at https://www.belfercenter.org/publication/national-cyber-power-index-2022.