UNIVERSITEIT iYUNIVESITHI STELLENBOSCH UNIVERSITY

1918 · 2018

saam vorentoe · masiye phambili · forward together

RESEARCH BRIEF 11/2019

Security Institute for Governance and Leadership in Africa

SIGLA @ Stellenbosch

Author: Ms N. Van der Waag-Cowling (SIGLA) **Series Editor**: Professor F. Vreÿ (SIGLA)

Africa must harness the potential of Cyber Power and Digital Diplomacy

Introduction

The year 2019 has witnessed major strategic shifts in the global cyber echo-system. Nation states are visibly competing with one another for cyber dominance and the quest to establish new international norms for state behaviour in cyberspace. New concepts such as cyber sovereignty, data nationalism and techplomacy are rapidly gaining traction in international relations. The potency of cyber power is now being fully realised and utilised as a strategic instrument by numerous states, in particular those with advanced economies and high cyber dependency. Africa is not isolated from cyber developments in general or immune to the resulting security ramifications and must adapt and participate more fully within the larger cyber system.

Discussion

At the core of cyberpower is the ability of a state to utilise its instrumentality to gain strategic advantage, both in the economic as well as the security spheres. Concomitantly, cyber or digital diplomacy can be effectually employed to leverage either soft or hard power and is becoming a mainstream feature of foreign policy. States in the global north are innovating rapidly in response to the shifting strategic landscape. By way of example, Australia and Denmark have appointed roving cyber ambassadors, Russia is pushing for the creation of a cyber general assembly at the United Nations and Estonia has created the world's first data embassies with full diplomatic immunity. Importantly, a key basis for cyberpower and defence lies in collective security, particularly in regions with many small states, for example, the European Union and NATO provide this multiplying effect to cyber capability within Europe.

Cyberpower is readily instrumentalised as a tool for the exercising of soft and hard power. While the hard power aspect is relatively straightforward in its application and relates to cyberattacks or even cyber-kinetic attacks, it is through the application of soft power that cyber can be used as a pervasive and potentially insidious tool. Africa appears to be slow in adapting to these new realities on a number of fronts and yet is it is poised to become one of the frontlines on which the global rivalry for cyber

ascendency will play out. The majority of African states do not give the impression that they view cybersecurity or cyberwarfare as a priority issue. It is in this apparent ambivalence that Africa appears to be out of step with the international order. Aside from the strategic implications of cyber threats, there are also the economic realities of cybercrime. It is estimated that on average, cybercrime costs states around 0.8% of GPD annually. If that is the case, then South Africa for example, with a 2019 First Quarter Gross Domestic Product growth of only 0.7% could technically be pushed into recession due to the cost of cybercrime alone. Given the poverty and security challenges on the African continent, the omnipotence of cyber threats have to be addressed.

The reasons for Africa's slow progress in most cyber-related matters are partly a mistaken belief that the continent has low internet penetration and that this therefore results in some level of cyber immunity. The opposite is in fact true, it simply equates to a target rich environment replete with low hanging fruit. A lack of technical capacity is hampering efforts to establish cyber resilience and capability, both of which are necessary foundations for the subsequent formation of cyberpower. Perhaps most concerning are the slow bureaucratic responses to securing cyber space. Finally there is the misperception that cyber incursions are principally aimed at monetary theft. Data is in fact the new currency and once stolen it is perpetual and can be repeatedly utilized and monetized. There are some exceptions as Mauritius, Rwanda, Kenya and Uganda are making progress and combining public/private partnerships to this end. Nigeria and South Africa, two of the continent's largest economies, should be leading the way. South Africa, in particular, has a rather advanced level of cyber dependency which increases vulnerability.

In order to understand the African cyber threat landscape, it is necessary to recognize the geopolitical realities which place the continent at the centre of rivalry between external powers for influence, resources, military presence and access to markets. There are numerous state and non-state actors participating in African conflicts which are also active in cyber space, including insurgent groups, private military companies and transnational terrorist groups. At times these protagonists act as proxies for other states. Some multinational companies conducting business in Africa also act as proxies for their governments. Then there are transnational organized crime groups, which via digital channels, have extended their operations on a global scale both for their own purposes and as proxy services. It is furthermore imperative that the link between social media and extremism be fully understood; "*the Information Age has witnessed a resurrection of ideology and increasing competition between narratives*." For Africa, a continent beset with conflict and weak states, ideology continues to remain a universal factor in driving conflict and accentuates the social media's utility.

Africa is additionally vulnerable as it imports virtually all of its information technology. Internet connectivity is growing at a rapid rate, yet the continent is ill prepared to face the hyper technology changes which are set to take place, namely 5G, quantum computing and artificial intelligence. These technologies will test cyber defences on a level which is not yet fully understood and an increasingly digitized Africa cannot avoid them. The key question is how will African governments respond to these strategic cyber threats? On the one level it entails building cyber capacity and developing fully articulated national cyber strategies. On another level, the answer lies in developing responses and capabilities on a diplomatic front and enhancing its own cyberpower. Collective cyber security is one such response. This is critical because it is only through collective security that Africa's limited research and development resources can be synergised in order to develop capacity, both human and technological. The African Union has been sluggish in providing adequate leadership in the cyber domain and African states are even slower. Only 14 of 55 African states have signed the AU Convention on Cyber Security and Personal Data Protection.

It is possible that regional entities such as ECOWAS and SADC may provide more common ground for cyber cooperation. They will, however, need to be more proactive in securing their collective cyberspace and hardening their systems. Cyber deterrence as a defence measure is reliant on attackers believing that there is sufficient evidence of the ability of states to respond to cyber-attacks. This is in turn reliant on the evidence of cyber capacity and research and development within states. Or to put it another way, the power of a state lies within the perception of its power. From a positive viewpoint, cyberpower provides the advantage of enabling a state to project greater power than its actual physical size and resources would otherwise allow. Small African states such as Rwanda, Benin and Mauritius which are showing innovation and a commitment to addressing their national cyber postures hold the potential to emulate Estonia, now dubbed "*Europe's little Technology Giant*" in harnessing digital technologies with the commensurate benefits.

Conclusions

Whilst the reality of building cyberpower capabilities in Africa will take substantial effort and resources in order to provide a yield in the future, the need for African states to engage in cyber diplomacy and ensure adequate foreign policy development in this domain must be addressed now. Cyber diplomacy should be utilised to ensure that African countries can determine outcomes to issues such as data sovereignty, pricing, access to information regarding criminals or terrorists using encrypted social media platforms, espionage, IP theft and control of critical information infrastructure. Africa is simply too dependent on technology within an increasingly digitized world not to ensure that its security concerns are addressed at the highest levels between states and on multilateral platforms. To this end, African countries need to ensure strong national public/private partnerships in order to drive their domestic security and technology agendas. What is of grave significance now, is that Africa signals its intent in meeting these challenges and assumes an immediate and visible posture in dealing with them.

Recommended Reading

1. Bebber, R.J, 'Cyber power and cyber effectiveness: An analytic framework', *Comparative Strategy*, Volume 36, Issue 5, pp 426-436, 2017.

2. Orji, *Multilateral Legal Responses to Cyber Security in Africa: Any Hope for Effective International Cooperation?* 2015. 7th International Conference on Cyber Conflict: Architectures in Cyberspace, M. Maybaum, A.-M. Osula, & L. Lindström (Eds.), 2015, NATO CCD COE Publications, Tallinn.

3. Rosenbach, E. & K. Mansted, The Geopolitics of Information. May 28, 2019. Available: https://www.belfercenter.org/index.php/publication/geopolitics-information

4. Segal, A. Chinese Cyber Diplomacy in a New Era of Uncertainty, Aegis Paper Series No. 1703, 2017.

5. World Economic Forum, *The 8 vital questions we need to address about international cybersecurity.* 2019. Available: https://www.weforum.org/agenda/2019/03/the-8-vital-questions-we-need-to-address-about-international-cyber-power-and-security/

Ms Noelle Van der Waag-Cowling is a lecturer in the Faculty of Military Science, researcher on cyber security in SIGLA and Associate Research Fellow/Centre for Conflict, Rule of Law and Society, Bournemouth University. She can be contacted at noelle@sun.ac.za