Stellenbosch UNIVERSITY IYUNIVESITHI UNIVERSITEIT
forward together
sonke siya phambili
saam vorentoe

RESEARCH BRIEF 4/2023

Security Institute for Governance and Leadership in Africa

SIGLA @ Stellenbosch

Authors: Karen Allen(Karen Allen International) **Series Editor:** Professor F. Vreÿ (SIGLA)

On cybersecurity in Africa: Building critical governance partnerships.

Introduction

If African states are to develop resilience against an increasingly pervasive cyber threat landscape, efforts to develop partnerships with key stakeholders will need to be dramatically ramped up and best practices shared. Those were among the key messages to dominate discussion at the Third International Workshop on Combatting Transnational Crime in Africa which focused on the continent's cyber security landscape. Put simply, in order to ensure that the continent does not become a "wild west" of cybersecurity, a phrase often used by some of the continent's foremost cyber experts. With more critical infrastructure attacks, ransomware intrusions and the weaponization of information on social media and messaging platforms, states need to become more proactive, and action orientated. Partnership building aligns with SDG 17 of the UN Sustainable Development Goals that tie in with Agenda 2063 of the African Union. To these ends actors must pool the knowledge, talent, expertise and capacity of government, academia, civil society, multilateral and regional organisations and the private sector to fortify their cyber defences. Furthermore, African states should consider engaging more actively, strategically and collectively with multilateral tech providers, as part of a growing trend towards "techplomacy" – a discipline of diplomacy that acknowledges the enormous power big tech companies have in helping to shape a new world order.

Discussion

Unlike other areas of technological development such as satellite technology, in which innovation has largely emerged from the defence and public sectors and was then adapted for civilian use (e.g., in the telecommunications industry), much of the current innovation in the cyber domain emanates from the private sector. This has implications for the proliferation, equitable distribution and governance or regulation of digital technologies.

Furthermore, it is primarily the private sector in the global north that is dominating how that technology is shaped, how algorithms are designed, how data is accessed, and how and where technology is diffused. Irrespective of this northern dominance, cyberspace has become a cornerstone of economic development with the African Union's digital transformation strategy underscoring the centrality of digitisation for the continent's economic development.

Moreover, the concept of a capable state hinges on a state's ability to leverage digital technology to carry out its key democratic functions whether it is ensuring the rule of law, maintaining defensive capabilities, securing the provision of critical services e.g., energy, water etc or ensuring citizens have access to information. While some states consider the cyber domain to be an extension of the nation-state reflecting a more securitised internet, others consider it a tool to assist in consolidating pillars of democracy by extending access to information. These conflicting views represent not only differing ideologies but also represent power relationships in respect of how the state engages with cyberspace and with the providers and innovators of digital technologies. Recent internet shutdowns on the continent in response to perceived threats to national security are an example of this.

Given the centrality of cyberspace in a new world order, African states arguably need to be at the table when issues of regulation, access and response are discussed. This is already happening with formations such as the GGE and OEWG in which there has been active participation by some African states. However, this engagement must be extended to include the technology giants, representing a significant shift towards a multistakeholder approach to governance and response. This more inclusive approach reflects the enormous power technology companies enjoy which consequently helps shape economies and the global security environment. It also reflects the reality that the cyber expertise, which state decision-makers must leverage to make informed decisions, primarily resides in the private sector.

A multistakeholder approach that draws in the private sector, academia and civil society also reflects a more human-centred view of cyberspace. It is not simply a technological discipline as cyberspace is a societal reality. Consequently, formations such as the G20 are incorporating issues of cyberspace and cybersecurity into their agendas. This more pluralist approach to setting the rules of the road for cyberspace also reflects the digital dependencies and complex power relationships, which overwhelmingly favour the most industrialised nations that cyberspace amplifies. African states undoubtedly need to be part of that conversation.

Furthermore, the African continent finds itself caught up in the geo-politics of technological competition. Two G20 countries dominate the emerging technology environment, and Africa is particularly vulnerable with respect to the infrastructure that underpins the digital system. This has been reflected in the debate about the Chinese provision of 5G technology in Africa which has been dominated by Chinese vendors and western concerns about surveillance norms becoming diffused in regions where China dominates technologically. There has been much discussion about Chinese tech companies providing CCTV technology. Questions raised include public space surveillance and facial recognition technology for the purposes of monitoring immigration and gaining access to state services in countries such as Kenya, South Africa and Zimbabwe and whether preferred norms are being exported along with the technology. These are some of the discussion areas where African states could offer a valuable contribution.

Capacity constraints within Africa resulting from competing policy priorities, economic development, organisational and legal challenges, human and technical capacity limitations provide further arguments for why Africa must step up its access to networks and partnerships to augment existing capacity, as well as clearly articulate Africa's needs and priorities in the cyber domain. While the workshop discussed whether African norms in cyberspace were distinctly different to global norms with active debates by participants, one delegate argued that it was a question of priorities rather than norms in Africa which may be different to those in other settings. One can see this for example in the areas of cyber terrorism and cybercrime including human trafficking and other forms of transnational crime enabled by cyberspace, which are perceived as main threats to Africa and the Middle East.

Furthermore, the underlying assumptions which inform global cyber policy and response frameworks may often fail to reflect the realities and constraints faced by many of the continent's 54 States. Therefore, African countries need to amplify their positions in multistakeholder engagements and build organisational strength.

High level intergovernmental formations such as the UN GGE and OEWG have sought to address some of the most pressing cyber issues by adopting non-binding cyber norms, but other initiatives such as Global Commission on Stability of Cyberspace, the Paris Call, the Global Forum on Cyber Expertise offer functional platforms for wider engagement among all cyber stakeholders.

The challenge for African leadership thus far has been to make the formations and platforms relevant to African challenges and priorities, and to leverage African engagement to support their capacity building efforts. One of the workshop delegates who also serves with the AU's cybersecurity body argued that African states "risk being caught out as unwary victims of Geo-politics". Therefore, African states need to build "proficiency in monitoring and navigating global economic commercial relationships" as they relate to cyberspace. Another delegate from the Africa Global Intelligence and Security Institute and who was instrumental in developing Ghana's 2016 National Cybersecurity Policy and Strategy, offered insights into the benefits of multistakeholder engagement. He demonstrated how Ghana has been something of a continental champion of the multistakeholder approach.

Organisationally Ghana's cyber security architecture is located in the ministerial and sub ministerial level across a range of government departments which also includes private sector players such as the banking sector. The central point of co-ordination is the cyber security authority. By integrating a comprehensive approach into all levels of Ghana's cybersecurity capabilities – including policy development, regulation and legislation, cross-border collaboration, capacity building, technical measures and other operational activities - the government has greatly enhanced its cyber resilience, and capacity to respond to cyber-attacks. It has also been able to leverage international partnerships through organisations such as ECOWAS and the Global Internet Forum to Counter Terrorism (GIFCT) to build capacity. Demonstrating a clear political will to work with private sector stakeholders has assisted Ghana's approach to building cyber resilience and offers a model which could be emulated more broadly.

Conclusion

By taking a proactive approach to cyber issues and adopting a broader multistakeholder approach, African states arguably can achieve two goals. They can better articulate the continent's (as well as their individual state's) cyber priorities, values and needs in a global environment and help shape the future direction of global cyber policy. Secondly, they can also use a broader engagement model to address key capacity constraints which may include cyber defence, situational awareness, response, mitigation, containment and recovery capabilities. While the state retains primacy over non-state actors with respect to decision making vis-à-vis national cyber policy, excluding the private sector as the shapers of the cyberspace of the future will surely only deprive the continent of valuable opportunities to harness the benefits of digital technologies and developing resilience to some of the threats.

Recommended reading

Ajijola AH and Allen N - "*African Lessons in Cyber Strategy*", Africa Center for Strategic Studies (8 March 2022)

Allen K – *Cyber Diplomacy and Africa's Digital Development*, Institute for Security Studies (Jan 2022)

Karen Allen is the Director of Karen Allen International, an Africa based consultancy which in addition to conducting research also provides communication tools to highlight issues of emerging technology.

Email: karen@karenalleninternational.com