INSTITUTE FOR SECURITY STUDIES

Cyber diplomacy and Africa's digital development

Karen Allen

Cyber diplomacy is the recognition that cyberspace is an environment in which digital superpowers and their proxies can project power and influence. African states must scale up their engagement to articulate clearly the continent's priorities. These priorities include driving rapid digitisation and ensuring they have the people, processes and skills to achieve the African Union's development objectives. The continent has much to gain from leveraging its demographic position as both a source of and a marketplace for future technology.

Key findings

- Cyber diplomacy seeks to establish a set of norms to regulate the behaviour of state and non-state actors in cyberspace. It also seeks to ensure that the developmental potential of digitisation is harnessed equitably.
- Competing policy priorities mean cyber diplomacy is often a 'nice to have' rather than an integral part of developing Africa's cyber capacity.
- The absence of continent-wide positions means Africa's cyber policies are often fragmented. 'Cyber champions' could streamline these policies.
- African states are often portrayed as 'junior partners' in cyber diplomacy discussions. This needs to change, given the rapid roll-out of tech on the continent and the targeting of African states by cyber criminals.
- Africa cannot afford to take a back seat in cyber diplomacy discussions, which are influential in shaping the design of digital technology and determining the rules for deploying it.
- Capacity and dialogue are necessary to future-proof technological innovation. Cyber diplomacy gives African states agency in shaping global digital priorities to meet Africa's needs. It also opens the doors to partnerships for skills development and knowledge transfer.
- Africa has much to gain from leveraging its position as an expanding marketplace for emerging digital technology as well as a source of indigenous innovation. These advantages should be used to ensure that the continent's priorities are articulated in multilateral discussions.

Recommendations

For the AU

- Recruit 'cyber champions': Africa must recruit 'cyber champions' from countries with high cyber maturity and internet penetration. These champions should seek to develop common continental positions on issues including freedom of expression.
- Uncouple trade negotiations from cyber diplomacy: The AU should encourage states to de-link trade issues from cyber diplomacy to allow for collective continent-wide approaches rather than the pursuit of individual short-term economic gains.
- Capacity and dialogue must be parallel processes to future proof technological innovation: African states cannot afford to wait until they reach higher levels of cyber maturity before engaging in cyber dialogue. The two must be parallel processes to enable the continent to have a say in how future technology is developed and policed.
- Increase digital capacity: Africa must increase digital capacity and not merely implement legislation. States should use private sector know-how to assist in building capacity, including diplomatic capacity.
- Demographic leverage: African states should leverage their relatively youthful populations to position themselves as a rapidly expanding future source of and marketplace for emerging technology. This would assist in ensuring their challenges are addressed as a global priority.
- Amplify Africa's position as an expanding market for emerging technology: The continent represents an expanding market for technological innovation. Consumer power should be leveraged to ensure cyberspace's 'rules of the road' reflect the continent's priorities, values and norms.

Introduction

Cyber diplomacy is the attempt by state representatives to establish a set of norms to regulate the behaviour of state and non-state actors in cyberspace. It also seeks to ensure that the developmental potential of rapid digitisation is harnessed equitably and fairly. It recognises that cyberspace is rapidly becoming a platform from which digital superpowers and their proxies, often referred to as 'hackers for hire',[1] can project power and influence.

This report seeks to identify key areas in which African states can leverage their position during these diplomatic engagements and ensure that the continent's digital priorities are met. It also sheds light on how the cyber engagements of Africa as a continent are viewed by 'outsiders' such as European diplomats.

Methodology

Given the limited academic literature on African cyber diplomacy, with some notable exceptions,[2] this report was informed by a series of closed expert roundtable discussions and bilateral meetings with experts, including government officials, academics, diplomats and members of civil society. It included engagements with diplomatic and technical representatives from leading cyber powers on the continent, including Mauritius, Kenya and South Africa, as well as those observing the continent from afar and representing foreign missions based in Africa.[3]

The report first identifies some of the key forums through which global cyber engagements take place. It then highlights the digital priorities of many African countries and identifies the challenges in ensuring that those priorities are articulated at a global level and seeks to identify key areas in which African states can leverage common positions by taking examples from other areas of foreign policy. It concludes by emphasising the need for a whole-of-government approach to cyber issues to inform international discussions.

Cyber diplomacy and power

States and their proxies exercise power in cyberspace by permitting or denying access to data, controlling infrastructure such as 5G networks and exerting influence by exporting norms such as those related to surveillance.

Another method is to manipulate artificial-intelligence-based technologies to sway public opinion at critical times such as elections – so-called information warfare or information operations.[4] In fragile democracies in which institutions such as the executive, the legislature and the judiciary may be weak, checks on the power of technology are especially critical.

Multilateral processes are in place to apply the rules-based order of international relations to cyberspace. The key forums include the UN's Group of Government Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security (GGE) and the Open-Ended Working Group on Developments in the Field of Information Telecommunications in the Context of International Security (OEWG).

Kenya, Mauritius, Morocco and South Africa have been represented on the GGE, which deliberates in private. It produced its final report in May 2021.[5] The OEWG draws on a broader range of participants, is considered more inclusive and is able to engage more broadly with industry actors, academia and civil society. The OEWG published its final report in March 2021[6] and has held a fresh round of meetings in December 2021.

In fragile democracies in which institutions may be weak, checks on the power of technology are especially critical

With respect to cybercrime, a Russian-sponsored UN Resolution has established an ad hoc committee to draft a new international cybercrime convention under the UN's Third Committee.[7] Algeria, Egypt and Nigeria will occupy office-bearing roles on that committee, which will hold its first substantive meeting in January 2022. Other multistakeholder initiatives, including the Global Commission on the Stability of Cyberspace,[8] have motivated for greater African representation and encouraged private sector engagement.

Cyber diplomacy has tended to revolve around the following key themes: cyber governance (rules and

norms), capacity building, response protocols and cybercrime. The agenda has been dominated by governance and protocols for responding to state-to-state cyber attacks.

One high-level regional official interviewed for this report observed that African interests are at times overshadowed because 'cyber superpowers view Africans as junior partners needed to make up the numbers in possible coalitions'. That point is contested by Western diplomats, who argue that 'it is imperative that Africans are aware of their strategically powerful position in agenda-setting and are also aware of the different global blocks.'

Although African states still trying to develop basic cyber capacity may consider cyber governance issues abstract and exclusive, people, processes and technology, capacity building and cyber governance are inextricably linked.

Capacity (including expertise, know-how, funding and time) helps to support the evolution of governance structures (or rules, laws and norms) that shape the possibilities and limits of future technological innovation. Expanding capacity should include developing the expertise to manage new forms of digital technology and understand their impact on society, both domestically and internationally.

People, processes and technology, capacity building and cyber governance are inextricably linked

African states cannot afford to be passive bystanders to essential discussions on cyber diplomacy – high-level multilateral discussions shape how states police and respond to digital intrusions and reflect the borderless nature of cyberspace.

The continent's leaders help set the rules for future generations. According to World Bank figures, by 2050 one in four of the world's people will come from sub-Saharan Africa.[9] The collective potential of African states to amplify their voice rests on the assumption that large numbers of digital consumers and producers will be in Africa.[10]

African priorities for African challenges

While the level of cyber maturity[11] of African states – their levels of infrastructure and capacity to withstand threats – varies considerably, there are compelling reasons for greater diplomatic engagement. Furthermore, some states should assume a more significant leadership role and become champions for the continent.

Capacity building

The African Union's Digital Transformation strategy, which aims to help stimulate economic growth, create jobs, eradicate poverty and 'ensure Africa's ownership of modern tools of digital management', strives for an 'integrated and inclusive' digital society by 2030'.[12] Kenya's development of the digital payments system M-Pesa is an example of the transformative nature of digital technology and showcases Africa's potential for further digital innovation.[13] Such advances should give African states the confidence to articulate their ambitions and concerns about rapid digitisation and push for greater inclusivity and access.

Technology design, values and norms

Human biases and norms underpin the way the technology we consume is designed. They inform the algorithms that power, for instance, social media platforms or biometric verification systems, which are increasingly used during elections, at borders and in public space surveillance.

Knowledge of algorithmic bias is growing fast. Data experts have highlighted that, unless checks and balances and global norms are in place, existing societal inequities and human rights abuses may be exacerbated.[14] Thus, African states need to be more proactive in helping to shape those norms.

Africa's development trajectory is increasingly driven by technological innovation in the fields of agriculture, education, finance and healthcare, among others. Experts observe that values and standards incorporated into emerging artificial intelligence (AI) technologies are potentially more suited to users in California than to those in Africa.

In light of the continent's diversity, it is debatable whether such an 'African standard' or 'value' exists and the most digitally developed states must engage in discussions

to determine rules for how that technology is developed and deployed.

Weaponised tech

Because technology can be weaponised in offensive operations, the cyber governance agenda has been prioritised in multilateral cyber discussions. Offensive operations are defined as research to identify potential adversaries' vulnerabilities, develop exploits[15] or build software tools and develop the human capacity to mount and manage offensive cyber operations.[16] The Council on Foreign Relations Cyber Operations Tracker, which monitors state-sponsored incidents, reports that since 2005, 34 countries have been sponsoring cyber operations.[17]

African states may experience collateral damage rather than being the primary targets of cyber attacks

The absence of cyber offensive abilities in most African countries, coupled with geopolitical alignments with traditional Western partners as well as Russia and China, may create a sense of neutrality, or at the very least, strategic balancing, among some states on the continent.

As a result, policymakers may feel that the likelihood of a state-sponsored cyber attack is remote. However, given that a number of government websites in the region have been hacked, this response is short sighted.[18] Global supply chains, too, have been disrupted by attacks.[19]

It is often difficult to find those responsible for attacks in cyberspace. Third parties frequently conduct state actions through so-called cyber mercenaries.[20] Thus African states may experience collateral damage as part of a broader geopolitical dynamic rather than being the primary targets.[21] The 'Anonymous' attack of 2016, which had an impact on some African countries, including South Africa, clearly demonstrated this.[22]

Many African states have fragile democratic institutions that are vulnerable to disinformation campaigns or information operations conducted by external state actors or their proxies. This has been observed particularly at critical moments, including election times, as documented in Kenya, Nigeria and South Africa.[23]

Western nations are investing substantial amounts to counter the potential threat of information operations in Africa.[24] The object is to reduce the risk of the continent becoming a weak link in efforts to police cyberspace.

Economic drivers

In 2021 a cyber attack on the South African state-owned enterprise Transnet, which operates the country's major ports, caused unprecedented disruption to the region's supply chains.[25] The ports handle freight transported beyond South Africa's borders into the Democratic Republic of Congo and Zimbabwe.

The Transnet hack was a sharp reminder that attacks on maritime targets appear to be increasing.[26] The ISS's Denys Reva has argued that in addition to implementing legislation within the maritime space, South Africa's future National Maritime Security Strategy must cover cyber security.[27]

Geopolitics and an 'arms race'

Another motivating factor for greater African engagement in cyber diplomacy relates to the ownership of emerging technologies and the inbuilt power relationships that accompany it. Adopting digital technologies is without doubt a development imperative. African states require the infrastructure that underpins the roll-out of digital technologies and the networks, hardware and other tools that define the cyber ecosystem. This makes them dependent on other state actors and their proxies.

However, the development agenda can bring unintended consequences. One example is the Sustainable Development Goals (SDGs) target 16.9, which seeks to guarantee 'a legal identity for all including birth registration.'[28] As a result, many African states have rolled out biometric databases to capture their population's details.

While such systems are potentially more efficient and may provide more equity for those individuals previously denied access to services based on identity documents or the lack thereof, they do raise questions of data security, sovereignty and dependence on technological superpowers.

Commentary on a cyber or big data 'arms race' highlights fears among some Western powers that China is seeking to dominate the cyber domain by controlling the systems, such as surveillance tools, that convey information.[29]

While French companies such as the tech multinational IDEMIA have a significant presence in West Africa, in other regions Chinese companies such as Huawei and Hikvision have succeeded in positioning themselves as more affordable than their competitors.[30] As a result, they are rapidly dominating the surveillance industry in Africa. This is reflected, for instance, in programmes to roll out so called 'smart cities' across the continent.[31]

Civil rights groups have warned of 'norm colonisation', cautioning that Chinese surveillance culture could influence domestic norms by stealth, including in Africa where checks and balances may be weak.[32]

The US and Europe are taking an increasingly harder line on big tech companies and the power they wield

For example, the proliferation of public space surveillance in South African cities has attracted the concern of civil society organisations, including Privacy International, which warns that surveillance culture will become all pervasive and entrenched as a norm.[33] There are also concerns that surveillance culture could give rise to more cyber espionage, both economic and political.[34]

In the United States (US) the 'arms race' in cyber and big data has triggered a decisive and drastic response. In 2019 President Donald Trump issued an executive order banning many foreign companies, including Huawei, from doing business in the country, citing concerns about 'sabotage' and risks to 'critical infrastructure'.[35]

Others followed suit, as the United Kingdom government banned telecoms providers from installing Huawei equipment in their 5G rollout, citing it as a 'high-risk vendor'.[36]

While African states have been relatively silent on this issue, experience on the continent may offer some salutary food for thought. The much-publicised data intrusion into the Chinese-built African Union building in Addis Ababa reported in 2012 has left a legacy of mistrust.[37] The West has used this to extend its influence, arguing that African states need to protect their data and the channels of access from states that have different privacy norms.

'Techplomacy'

As powerful technology companies have expanded, scholars and policymakers have recognised the need to create opportunities for the private tech sector and governments to engage.

An emergent sub-set of cyber diplomacy, dubbed 'Techplomacy', seeks to 'institutionalise' responses to an increasingly influential global sector, to exert pressure on the tech giants to behave 'responsibly'.[38]

Many of the big tech companies are based in the US and arguably lack context or a nuanced understanding of the norms, culture and sensibilities of other countries. Instead, they have the potential to project values reflecting those of the territories in which their headquarters are based, which, in most cases, is the US.

The US and Europe are taking an increasingly harder line on the big tech companies and the power they wield, introducing regulations aimed at curbing their monopoly power, their erosion of privacy and the spread of mis/disinformation.[39]

The debate about the limits to social media freedoms in Africa and, in particular, internet shutdowns in countries such as Nigeria and Ethiopia, reflects this wider global trend towards curtailing the power of tech. Some African states are now considering legislation that will oblige social media firms to locate offices within local jurisdictions, which would exert pressure on them to comply with domestic laws.[40]

Africa has a contribution to make to such discussions in future from both a consumer protection and an international relations standpoint. What was hitherto claimed by the tech companies to be their 'net neutral' position is now being challenged by governments in the global north. One example is the US congressional hearings on issues such as how social media companies such as Facebook use personal data and, more recently, questions about how the social media giant deals with child safety online.[41]

Given Africa's relatively youthful population, which will present a rapidly expanding future source and marketplace for emerging technology, the continent is well placed to assert its views in such discussions.

Battle for norms

The fact that there have been two bodies involved in developing norms partly reflects geopolitical competition in the cyber domain, with African interviewees speaking of the tussles for influence among rival cyber superpowers during multilateral engagements.[42]

Both the GGE and the OEWG aim to agree on a set of norms, in effect soft laws, governing the behaviour of states in cyberspace, including consensus about the fact that, broadly speaking, international law is applicable. In its latest report the GGE agreed to a set of 11 such norms.[43]

The primary vectors for intrusions include cyber espionage, critical infrastructure sabotage and transnational organised crime

However, other issues, including those relating to the attribution of cyber attacks, are deemed more controversial and divide opinions along geopolitical lines.[44] At the time of writing a resolution before the UN General Assembly, co-sponsored by the US and Russia, seeks to harmonise the two processes.[45]

Africa and cybercrime

In light of Africa's particular vulnerability to cybercrime it is imperative that the continent engages in cyber diplomacy.[46] With estimates that cybercrime could cost the global economy US$10.5 trillion by 2025, international efforts are under way to scale up capacity in Africa to mitigate its effects through partnerships and practical training.[47]

The primary vectors for intrusions include cyber espionage, critical infrastructure sabotage and transnational organised crime. In African states with more advanced economies and financial infrastructure, such as South Africa, Kenya and Ghana, attacks on computer infrastructure are increasing rapidly.[48] So, too, is the use of the internet to commit traditional crimes such as extortion, fraud, and human trafficking.

Two key instruments seek to build cooperation. They are the Convention on Cybercrime of the Council of Europe, known as the Budapest Convention, and the African Union Convention on cyber security and personal data protection, the Malabo Convention.[49]

However, in both cases there has been a problem securing African buy-in. Broadly speaking, some African states consider the Budapest Convention to be a 'foreign' regional instrument, while the Malabo Convention has

US$10.5 trillion

ESTIMATED COST OF CYBERCRIME TO GLOBAL ECONOMY BY 2025

failed to secure widespread ratification, despite being a continental creation.[50] This is partly because many African states have struggled to enact the domestic legislation and regulations required to make key parts of the treaty work.

The vague and ubiquitous term 'capacity building' must be interpreted more widely to incorporate practical skills development, not simply the generation of legislation, which states often find hard to implement.[51] It requires training and empowering lawyers, civil society, policymakers and other stakeholders to articulate the continent's priorities in multilateral discussions.

Capacity building should also include diplomatic capacity. A new generation of African cyber diplomats is gradually evolving to address this skills gap. This process must be scaled up.

States should adopt a whole-of-government approach to cyberspace and not view it as just a technical issue

In addition, there is a drive to make cyber discussions more representative. For example, there are initiatives to include more women in cyber mentoring programmes to address the broader issue of gender imbalances in disarmament forums and to extend the themes discussed in international forums.[52]

Private sector engagement in multistakeholder efforts is increasingly being actively encouraged on the basis that much of the expertise resides in that sector. Formations such as the Global Commission on the Stability of Cyberspace are driving efforts to scale up private sector capacity building and engagement and include voices from this sector in wider global cyber discussions.[53]

African states should adopt a whole-of-government approach to matters of cyberspace and not simply view it as a technical issue. A major challenge confronting many African governments is the absence of policy coherence. The development of African cyber diplomats may go some way to addressing this by identifying priority areas for action. However, these highly trained diplomats must exert influence beyond their foreign affairs ministries and should be deployed as cyber ambassadors and a knowledge resource throughout government.

It is not just security and crime clusters that should be engaged, cybersecurity issues and positions on cyber norms should be aligned across government. One analyst suggested that in the future the notion of a 'capable state' will hinge on its digital as much as its physical capacity.

Leveraging Africa's position in cyber diplomacy

Existing geopolitical alliances may influence the cyber engagements of the 54 African members of the UN. However, the sheer strength of numbers offers some leveraging power within the UN General Assembly, which has mandated the GGE and OEWG processes.

Africa has a huge stake in helping to shape the 'rules of the road' for new and future digital technologies. Given the continent's population growth projections it is reasonable to assume that it will constitute a rapidly expanding market for these technologies.

The continent's most developed cyber states collectively constitute an important block in terms of both votes and influence. The biggest challenge, or potential opportunity, for regional bodies such as the African Union is to convert this into organisational strength. An ISS report on common African positions on global issues stated that 'negotiating common African positions (CAPs) in the African Union (AU) system is convoluted, politically stressful and difficult.'[54]

It identified resource shortages within the AU and warned that 'human skills and knowledge of CAP themes are lacking'. Given the AU's commitment to its Digital Transformation Strategy there is an urgent need to address these shortfalls within the cyber diplomacy domain and elevate digital literacy issues among lawmakers and policymakers.

As one cyber diplomat observed:

> The AU is well placed to try to seek common positions, and it has legitimacy. Yet countries such as Kenya, South Africa, Nigeria, and Mauritius are all working in isolation. We need to create forums that allow African states to thrash out those discussions so that they can go into multilateral talks with common positions.

Regional cyber dialogues are already seeking to identify areas of shared understanding. Still, there is an urgent need to move digital issues higher up the political agenda and overcome competition for limited government time and resources.

Africa's commitment to balancing geopolitical interests strategically will be tested at the Ad Hoc Committee meetings scheduled to be held in January 2022. At the time of writing Russia, Kuwait and Oman have already presented submissions in what some commentators believe is an attempt to try to control the agenda.[55]

Furthermore, rights groups have raised concerns that the key drivers of this committee are seeking to redefine what constitutes a cybercrime in ways that may encroach upon democratic values such as freedom of expression.[56]

The extent to which African states push back collectively against some of the 'pre-cooked' recommendations before the meetings have even begun will be an important test of African agency. In particular, South Africa's role as a constitutional democracy that champions human rights could position the country to be more robust in leading resistance to norms that challenge these rights.

The AU should encourage African states to de-link trade issues from cyber diplomacy dialogue

European cyber diplomats have urged their African counterparts to seek like-minded alliances to leverage African agency. However, African officials in the field say they are often considered simply as junior partners in such formations. The absence of Africa-wide positions on many of the cyber related issues mentioned above has been an impediment to engaging as a regional block and adopting a more assertive posture in such discussions. Therefore, a more effective strategy may be for the continent's cyber champions to identify points of convergence with cyber powers on specific human rights, privacy and security rather than buying into a wholesale cyber ideology.

Where possible the AU should encourage African states to de-link trade issues from cyber diplomacy dialogue. This will enhance the likelihood of continent-wide positions being adopted rather than states pursuing short-term economic gains founded on bilateral relationships.

There has been much discussion about the dependency and vulnerability of African states such as Zimbabwe on cyber superpowers such as China, which are providing important digital infrastructure that will potentially transform their economies. As part of the commercial arrangements the vendors have access to Zimbabwe's data, which it may be used for further product development or, as some fear, as a tool of repression by Zimbabwe or surveillance by China.[57]

Conclusion

The phrase the Fourth Industrial Revolution is loudly trumpeted by many African governments and presented as a panacea for development challenges. Yet without fully understanding the opportunities as well as the unintended consequences that accompany digital innovation Africa risks being left behind in setting the rules of cyberspace.

Engagement in cyber diplomacy must be entrenched in the continent's wider strategy to bridge the digital divide. If capacity-building efforts do not go hand in hand with international engagement, Africa's priorities might be overshadowed by wider geopolitical and governance concerns.

As important as international cyber diplomacy is the need for a whole-of-government approach to cyber issues, building understanding and adopting a human-centred approach to international cyber engagement.

The more digitally developed African states should become 'cyber champions', seeking to achieve common continental positions ahead of major multilateral engagements. Countries such as South Africa, Kenya, Mauritius and Nigeria have both the human and political capital to lead the charge on behalf of the continent and elevate Africa's voice in critical cyber discussions. However, such 'cyber champions' must be closely monitored by their peers to avoid them becoming gatekeepers, influenced by their own bilateral trade relations with cyber superpowers.

Notes

1 '*Hackers for Hire in West Africa*', Amnesty International, 2021, www.amnesty.org.uk/files/2021-10/FINAL-%20Hackers-for-Hire%20in%20West%20Africa.pdf?VersionId=Z9PiZVsLbKa6_oR_verh5U_iC0RXqJm6; D Reva, 'Maritime cyber security getting Africa ready', *ISS Today*, October 2020.

2 https://issafrica.org/research/africa-report/maritime-cyber-security-getting-africa-ready; D Reva, 'Africa can't risk a major maritime attack', *ISS Today*, October 2020, https://issafrica.org/iss-today/africa-cant-risk-a-major-maritime-cyber-attack.

3 The opinions of nearly 20 experts in the African cyber diplomacy space helped to inform these recommendations and the ISS thanks those who participated for their time.

4 E Pauwels, *Anatomy of Information Disorders in Africa*, Konrad Adenauer Stiftung, 9 September 2020, www.kas.de/en/web/newyork/single-title/-/content/the-anatomy-of-information-disorders-in-africa.

5 *Report of the Group of Government Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security*, UN Office for Disarmament Affairs, 28 May 2021, https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf.

6 *Open ended working group on developments in the field of information and telecommunications in the context of international security – Final Substantive Report*, UN Office of Disarmament Affairs, 10 March 2021, www.un.org/disarmament/open-ended-working-group/.

7 Ad Hoc Committee established by General Assembly Resolution 74/24, UN Office on Drugs and Crime, www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home.

8 Global Commission on the Stability of Cyberspace, https://cyberstability.org.

9 E Suzuki, 'World's population will continue to grow and will reach nearly 10 billion by 2050', World Bank Blog, 2 July 2009, https://blogs.worldbank.org/opendata/worlds-population-will-continue-grow-and-will-reach-nearly-10-billion-2050.

10 Ibid.

11 J Christopher, 'The Cybersecurity Maturity Model: A Means to Measure and Improve Your Cybersecurity Program', Forbes, November 2018, www.forbes.com/sites/forbestechcouncil/2018/11/01/the-cybersecurity-maturity-model-a-means-to-measure-and-improve-your-cybersecurity-program/?sh=1161312d680b.

12 'The Digital Transformation Strategy for Africa 2020-2030', African Union, 18 May 2020, https://au.int/en/documents/20200518/digital-transformation-strategy-africa-2020-2030.

13 Vodaphone.com, www.vodafone.com/about-vodafone/what-we-do/consumer-products-and-services/m-pesa.

14 'Overcoming AI bias to empower an equitable society', Global Government Forum, 25 August 2021, www.globalgovernmentforum.com/overcoming-ai-bias-to-empower-an-equitable-society/.

15 An exploit is a code that takes advantage of a software vulnerability or security flaw.

16 W De Sombre, M Campobasso, L Allodi, J Shires, JD Work, R Morgus, P Howell O'Neill and T Herr, A primer on the proliferation of offensive cyber capabilities, Atlantic Council, 1 March 2021, www.atlanticcouncil.org/in-depth-research-reports/issue-brief/a-primer-on-the-proliferation-of-offensive-cyber-capabilities/.

17 Cyber Operations Tracker, Council on Foreign Relations, www.cfr.org/cyber-operations/.

18 Y Pillay, 'Justice Department Recovering after IT services hacked', *IOL News*, 12 October 2021, www.iol.co.za/mercury/news/justice-department-recovering-after-it-services-hacked-a4f78365-8914-4073-8d34-76424a448292.

19 D Reva, 'Cyber attacks expose the vulnerability of south Africa's ports', *ISS Today*, 29 July 2021, https://issafrica.org/iss-today/cyber-attacks-expose-the-vulnerability-of-south-africas-ports.

20 'IT security threat warning for South Africa – hackers for hire', *Business Tech*, 24 October 2020, https://businesstech.co.za/news/trending/442318/it-security-threat-warning-for-south-africa-hackers-for-hire/.

21 D Reva, 'Cyber attacks expose the vulnerability'.

22 B van Niekerk, 'An analysis of cyber-incidents in South Africa', *The African Journal of Information and Communication* 20, 2017; www.scielo.org.za/scielo.php?script=sci_arttext&pid=S2077-72132017000100006; D Reva, 'Cyber attacks expose the vulnerability'.

23 Pauwels, *Anatomy of Information Disorders*.

24 www.rand.org/topics/information-operations.html.

25 Z Shabalala and T Heiberg, 'Cyber-attack disrupts major South African Port Operations', *Reuters*, 22 July 2021, www.reuters.com/world/africa/exclusive-south-africas-transnet-hit-by-cyber-attack-sources-2021-07-22/.

26 I Booth, 'Transnet cyberattack could have catastrophic consequences', *Investec Focus*, 28 July 2021, www.investec.com/en_za/focus/economy/transnet-cyberattack-could-have-catastrophic-consequences.html.

27 Reva, 'Cyber attacks expose the vulnerability'.

28 *The Human Rights Guide to the sustainable development goals*, The Danish Institute for Human Rights, https://sdg.humanrights.dk/en/targets2?target=16.9.

29 'Big Data a twenty-first century arms race', Atlantic Council and Thomson Reuters, 27 June 2017, www.atlanticcouncil.org/in-depth-research-reports/report/big-data-a-twenty-first-century-arms-race-2/.

30 'The importance of "identity for all" for the development of nations', *Idemia*, 16 October 2021, www.idemia.com/news/importance-identity-all-development-nations-2021-09-16.

31 E Siba and M Sow, *Smart City Initiatives in Africa*, Brookings, 1 October 2017, www.brookings.edu/blog/africa-in-focus/2017/11/01/smart-city-initiatives-in-africa/.

32 S Allison, 'Cameras will make you safe', *Mail & Guardian*, 15 November 2019, https://mg.co.za/article/2019-11-15-00-our-cameras-will-make-you-safe/.

33 https://privacyinternational.org/explainer/1632/global-surveillance-industry; for a broader discussion on surveillance colonisation see S Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, Profile Books, 2019; 'The city surveillance state inside Johannesburg's safe city initiative', SAIIA, 15 March 2021, https://saiia.org.za/research/the-city-surveillance-state-inside-johannesburgs-safe-city-initiative/.

34 L Jinghua, *What are China's cyber capabilities and intentions?*, Carnegie Endowment for International Peace, 1 April 2019, https://carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intentions-pub-78734.

35 H Simonds, 'Trump signs order effectively banning Huawei telecom equipment in US', *Android Authority*, 16 May 2019, www.androidauthority.com/huawei-equipment-ban-987000/.

36 'Big Data a twenty-first century arms race'; 'Britain bans new Huawei 5G kit instillation from Sept 2021', *Reuters*, 30 November 2020, www.reuters.com/article/us-britain-huawei-idUSKBN28A005.

37 A Maasho, 'China denies report it hacked African Union Headquarters', *Reuters*, 29 January 2018, www.reuters.com/article/us-africanunion-summit-china-idUSKBN1FI2I5.

38 'Introducing Techplomacy: A roundtable with Denmark's tech ambassador Casper Klyne', Brookings India, November 2018, www.brookings.edu/wp-content/uploads/2018/11/IntroducingTechplomacy.pdf.

39 'A global tipping point for reining in tech has arrived', *New York Times*, 20 April 2021, www.nytimes.com/2021/04/20/technology/global-tipping-point-tech.html.

40 The Kenya Information and Communications (Amendment) Bill 2019, www.bowmanslaw.com/wp-content/uploads/2019/10/Kenya-Information-and-Communication-Amendment-Bill-2019-No.2_compressed.pdf; In Nigeria, The Protection from Internet Falsehoods, Manipulations and Other Related Matters Bill 2019, https://placng.org/i/wp-content/uploads/2020/03/Protection-from-Internet-Falsehood-Bill-Summary.pdf.

41 'Facebook Social Media Privacy, and the use and Abuse of Data', US Congress, 10 April 2018, www.congress.gov/event/115th-congress/senate-event/LC64510/text?s=1&r=59; 'Protecting kids online: Testimony from a Facebook Whistleblower', US Senate Committee on Commerce Science and Transportation, 5 October 2021, www.commerce.senate.gov/2021/10/protecting%20kids%20online:%20testimony%20from%20a%20facebook%20whistleblower.

42 https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/465/01/PDF/N1846501.pdf?OpenElement.

43 'Report of the group of government experts on Advancing responsible State behaviour in cyberspace in the context of international security', UN Office for Disarmament Affairs, 28 May 2021, https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf.

44 https://dig.watch/processes/un-gge#view-7541-4.

45 'ICT4 Peace Welcomes new UN joint resolution on peace and security in cyberspace – But concerns remain, https://ict4peace.org/activities/ict4peace-welcomes-new-un-joint-resolution-on-peace-and-security-in-cyberspace-but-concerns-remain/.

46 N Allen, 'Africa's Evolving Cyber threats', Africa Center for Strategic Studies, 19 January 2021, https://africacenter.org/spotlight/africa-evolving-cyber-threats/.

47 Ibid.

48 'INTERPOL launches initiative to fight cybercrime in Africa', Press Release, 12 May 2021, www.interpol.int/en/News-and-Events/News/2021/INTERPOL-launches-initiative-to-fight-cybercrime-in-Africa.

49 'Budapest Convention and Related Standards', www.coe.int/en/web/cybercrime/the-budapest-convention; 'African Union Convention on Cyber Security and Personal Data Protection', https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.

50 At the time of writing just eight African states had ratified the treaty. They are Angola, Ghana, Guinea, Mozambique, Mauritius, Namibia, Rwanda and Senegal.

51 In South Africa the Protection of Personal Information Act and the Cybercrimes Act have both fallen victim to the challenges of implementation and a lack of urgency.

52 L Sharland, N Goussac, E Currey, G Feely and S O'Connor, 'System Update: Towards a Women, Peace and Cybersecurity Agenda', United Nations Institute for Disarmament research, 2021, www.unidir.org/sites/default/files/2021-09/UNIDIR_System%20Update.pdf.

53 Global Commission on the Stability of Cyberspace, https://cyberstability.org.

54 B Adeoye, 'Common African positions on Global Issues: Achievements and Realities', Institute for Security Studies, December 2020.

55 First Session of the Ad Hoc Committee, UN Office on Drugs and Crime, 17–28 January 2022, www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-first-session.html.

56 D Brown, 'Cybercrime is dangerous but a new UN Treaty could be worse for rights', Human Rights Watch, 13 August 2021, www.hrw.org/news/2021/08/13/cybercrime-dangerous-new-un-treaty-could-be-worse-rights.

57 A Hawkings, 'Beijing's Big Brother Tech Needs African Faces', *Foreign Policy*, 24 July 2018, https://foreignpolicy.com/2018/07/24/beijings-big-brother-tech-needs-african-faces/.

About the author

Karen Allen, who has a Master's degree in international relations and contemporary war from King's College London, is a Consultant at the ISS in Pretoria. She joined the ISS in June 2019 as senior research advisor: emerging threats in Africa, in the office of the executive director. She is a Visiting Fellow in the Department of War Studies, King's College London.

About ISS Africa Reports

The Africa Report series analyses human security problems and solutions at the regional and continental level. It also considers the implications and lessons from Africa for global policy. Reports provide insights into African and global policy on conflict trends, conflict prevention, peacebuilding, terrorism, organised crime, peace operations, maritime security, migration, development and governance.

About the ISS

The Institute for Security Studies (ISS) partners to build knowledge and skills that secure Africa's future. The ISS is an African non-profit with offices in South Africa, Kenya, Ethiopia and Senegal. Using its networks and influence, the ISS provides timely and credible policy research, practical training and technical assistance to governments and civil society.

Development partners

The ISS is grateful for support from the members of the ISS Partnership Forum: the Hanns Seidel Foundation, the European Union, the Open Society Foundations and the governments of Denmark, Ireland, the Netherlands, Norway and Sweden.

ISSN 2617-7749 Print
ISSN 2617-7757 Digital