Unpacking Cyber-Capacity Building in Shaping Cyberspace Governance: the SADC case

Enrico Calandro, Ph.D., ecalandro@researchictafrica.net

Nils Berglund, nberglund@researchictafrica.net

Abstract

Issues around safety and security of cyberspace in Africa need to be located in their own specific political economy and Internet ecosystem as it manifests itself in various African jurisdictions and at a regional and sub-regional level. Technically, the Internet in Africa is based on similar standards and protocols developed by technical international bodies such as ICANN, the IETF and the W3C – generally with low or ineffective participation of African stakeholders. Nevertheless, the network is characterised by lack or under-utilisation of physical resources such as IXPs, dearth of local content, poor quality of service, high price and high level of latency, and by an irrelevant number of domain names registrars serving an absent or nascent Internet industry. Although African countries have not yet achieved satisfactory levels of digitalisation to attain the UN Sustainable Development Goals, it does not imply that they are not vulnerable to the new forms of risks and threats that exist in cyberspace. The resource-constrained setting of Sub-Saharan Africa characterised by little awareness of cybersecurity risks and transactions, from a user perspective may have an impact on security decisions. Many of these users are novices with little awareness of mobile security risks and with little or no protection, as transactions are often computed in countries without or with nascent cybersecurity and data protection legislation. This has resulted in Africa being a continent with one of the highest rates of cybercrime affecting the strategic, economic and social growth development of the region. A different but related challenge in protecting people's rights in cyberspace is Africa's readiness to develop and enforce cybercrime and data protection laws. According to UNECA, African governments are demonstrating increasing awareness of cybersecurity issues, but existing capability to deter, monitor or pursue cybersecurity has been ineffective. Rather, cybersecurity concerns in response to a widespread diffusion of mobile connectivity, have often been addressed with mass surveillance measures in Africa. Building and understanding African governments' cyber policy readiness and capacity and promoting citizens' trust in cyber realms are therefore pressing concerns for the state and non-state actors dealing with building cyber capacity in Africa.

To respond to emerging threats and risks in the cyberspace, capacity building has emerged in international cybersecurity policy debates and practise as a possible remedy for developing countries to cope with an increasing cyber threat. Globally, epistemic communities have developed norms and "best practices" that are introduced to developing countries mostly through capacity building and technical assistance by multilateral organisations. Yet, democratic assumptions about human rights, freedom of expression, privacy, and security that inform policies and regional frameworks of the European Union and its like-minded allies often collides with the political economy of fragile African democratic states, and with their under-resourced institutional arrangements, which often lack necessary technical skills and financial resources to effectively implement reforms.

By mapping cyber policy frameworks as an output of cyber capacity programmes in a sub-region in Africa (SADC), the study argues that in addition to lack of capacity and uneven ICT development across SADC countries, other reasons for poor implementation of global and regional cyber policies, protocols and declarations are related to lack of coordination between (sometimes) competing global and

regional agendas, and between cyber capacity activities aiming at implementing such frameworks. Despite the existence of national, regional and international human rights instruments that acknowledge privacy, freedom of expression and access to information as fundamental human rights in African jurisdictions, what is observed at a national level is that a number of SADC governments are implementing measures that rather than protecting people from cyber-threats and privacy violation through cybersecurity and data protection legislation, restrict Internet access and use, for instance during election time (shutting down the net), via social media taxes, or via mass surveillance.

In the conclusions, the paper suggests that rather than pursuing legally binding international treaties on the governance of cyberspace, which would place additional implementation and enforcement requirements on fragile and incapacitated states with weak institutional arrangements, better collaboration between different stakeholders dealing with cyber capacity is needed for capacity building programmes to be effective.

Keywords: SADC, cyber capacity, cyber diplomacy, regionalism.

Introduction

As risks have continued to grow in tandem with the development of the Internet, cyberspace has become a new domain of global security affairs. The international debate on the governance of cyberspace, characterised by multilateralism and rules-based international order, has been checkered with repeated calls for a global consensus on cybersecurity. Perhaps the most notable effort towards such a consensus has come in the form of the Council of Europe Convention on Cybercrime, also called the Budapest Convention, which pursued a "common criminal policy aimed at the protection of society against cybercrime, *inter alia*, by adopting appropriate legislation and fostering international co-operation" (CoE, ETS 185 – Convention on Cybercrime, 23.XI.2001, 2011). Appeals to this effect are characteristic among a wide range of other stakeholders in the sector. For example, the UN Group of Governmental Experts (UN GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, along with the recently established Open-Ended Working Group (OEWG), are working towards an international framework on 'responsible state behaviour in cyberspace' (GIP Digital Watch Observatory, 2019a). Similar emphasis on the need for a globally consistent cybersecurity approach have been articulated in academia (Sund, 2007) (Schjølberg & Ghernaouti-Hélie, 2009) (Arimatsu, 2012) (Ariu, et al., 2016), by the private sector, and in the policy agendas of several nations. One of the three key elements of the United States International Cybersecurity Strategy, for example, is "the development of an international consensus on and promotion of additional voluntary norms of responsible state behavior in cyberspace that apply during peacetime" (Painter, 2016). Meanwhile, Microsoft has declared the need for a 'Digital Geneva Convention' and supported the Paris Call for Trust and Security in Cyberspace (Smith, 2017) (2018), and Siemens, in collaboration with the Munich Security Conference and other partners, are promoting their own international Charter of Trust, which aims to, "develop and implement rules for ensuring cybersecurity throughout the networked environment" (Breuer & Webel, 2019).

Building towards consensus has also been a priority at regional and sub-regional levels. The International Telecommunications Union (ITU) and the World Bank have produced model laws in regions like the Southern African Development Community (SADC) (ITU, 2013a) and the Organisation of Eastern Caribbean States (World Bank, 2016), with the aim of harmonising cybersecurity legislation in the respective regions. The BRICS bloc has also discussed a unified approach to securing cyberspace, stating, "We will explore cooperation on combating cybercrimes and we also recommit to the negotiation of a universal legally binding instrument in that field" (BRICS, 2014). The African Union (AU), for its part, launched the AU Convention on Cyber Security and Personal Data Protection, also called the Malabo convention of 2014, in collaboration with the UN Economic Commission for Africa (UNECA), with similar intentions of unifying the continent under the same rules and priorities (African Union, 2014).

Despite these calls and efforts of civil society organisations (CSO), national governments, regional economic communities, the private sector, academia, and technical communities, an effectively global consensus has proved elusive (Gold, 2019). While calls for consensus itself are practically ubiquitous, the particularities of the approaches to, and priorities of cybersecurity policy and strategy can considerably diverge, both nationally and regionally, and between the public, the private, and CSO sectors. Disagreements on the governance of cyberspace have been significant since at least 1998, when the Russian Federation brought forth a General Assembly resolution on information security

(A/53/PV.79, 1998). The approach to cybersecurity advocated by Russia, largely shared by the broader Shanghai Cooperation Organization and several other countries, continues to differ from that of the European Union and its like-minded allies, along lines of state control, the role of the ITU, and human rights in cyberspace (Nocetti, 2015) (Pawlak, 2016).

The 2012 World Conference on International Telecommunications (WCIT) featured a notably contentious debate on whether to expand the mandate of the ITU to Internet governance functions, thus purportedly expanding government influence over the Internet, an issue that resulted in a clear division between the EU, OECD and Freedom Online Coalition members against the treaty, and comparatively less democratic states[1] voting in favour (Maurer & Morgus, 2014). In the case of BRICS, there has been agreement on expanding the role of the United Nations (Panova, 2015), but approaches to cybersecurity differ significantly among the five members (Kshetri, 2015), and a unified approach or agreement has yet to emerge. Other roadblocks to global consensus include cyber disarmament, promoted by some European states but contested by the United States (Arimatsu, 2012) as well as concepts like 'information sovereignty' (Nocetti, 2015). Caught at the nexus of differing opinions, some African nations with more capacity and regional influence, including Botswana and South Africa in SADC, have been characterised as 'swing states' (Maurer & Morgus, 2014) in global cyber policy controversies. As such, ongoing discussions on cyberspace and Internet governance can be understood as *fora* in which the agendas and worldviews of nations strategically compete for influence (Nocetti, 2015). Most recently, however, a resolution brought forward by the Russian Federation at the UN General Assembly's Third Committee in November 2019, entitled, "Countering the use of information and communications technologies for criminal purposes" (A/C.3/74/L.11, 2019) received notable support from Southern Africa nations, with eight states in favour, three abstaining, and none siding against out of 16 SADC member states.

The efforts by multilateral organisations to promote versions of a global consensus through norms, best-practices, technical standards, or rules and priorities, often take the form of capacity building projects (Calandro, 2015). The United Nations originally defined capacity building as a means to, "invent, develop and maintain institutions and organisations that are capable of learning and bringing about their own continuing transformation, so that they can better play a dynamic role to sustain national development processes" (E/2002/58, 2002, p. 4). These are typified by workshops on policy and strategy, technical training, or model laws. Specifically, in the context of cybersecurity, 'capacity' is a broader term that can be understood as a state's ability to effectively manage the functions necessary for securing cyberspace. In this sense, capacity building is a mechanism that can refer to a number of projects promoted and implemented by a multitude of stakeholders. The UN GGE report 2015 emphasises that states need to "provide assistance and training to developing countries to improve security in the use of ICTs" ((A/70/174, 2015) para 21 (b)). In that context, the term "can mean anything from the development of cybersecurity policies and legislation, to law enforcement capacity and public cybersecurity awareness campaigns" (Kumar, 2019). Whatever their shape, the dominant narrative around capacity building is that in addition to development goals, they promote international collaboration, information sharing and serve as mechanisms to build a global consensus on the issue of cybersecurity. Although not only developing economies are the addressees of capacity

[1] "Less democratic" in this case is based on the metrics of the 'Freedom in the World Index' (Freedom House, 2018) and the Democracy Index of the Economist Intelligence Unit (The Economist, 2018).

building measures (Homburger, 2019), forms of donor-recipient relationship exists in cyber capacity building (Muller, 2015).

Pawlak's (2016) understanding of capacity building as 'an instrument for foreign affairs' recognises that the activities of donor nations and organisations like the ITU or the Council of Europe may have agendas beyond the socioeconomic development of their recipients, a view consistent with other perspectives in critical scholarship (e.g (Hameiri, 2009) (Kaldor, Martin, & Selchow, 2007) (Saran, 2016)). In this sense, different approaches to cybersecurity governance can be promoted through cybersecurity capacity building as the latter implies a transfer of values and world views from the donor countries (Hurwitz, 2014; Nunnenkamp, 1995). More than a neutral endeavour, then, capacity building is also a "foreign policy tool used to advance national interests (ideological, security, economic, etc.) and norms" (Pawlak, 2016, p. 85). This is based on the assumption that the broader purpose or end goal of capacity building activities in cybersecurity is at least in part to coordinate a congruence of norms and values that are consistent with the priorities of the actor that undertakes them. In the case of the Council of Europe for example, this process materialises in an emphasis on the multistakeholder approach and their advocacy for a human-rights-based framework for Internet governance, promoted across Africa and elsewhere (Pawlak, 2016).

Pawlak's framework for understanding capacity building as an instrument for foreign affairs can also be extended beyond the efforts of nations, donors or multilateral organisations like the Council of Europe and the ITU, to include the priorities of the private sector in international cybersecurity debates. Multinational corporations have consistently called for their own image of a global consensus on approaches to cybersecurity, which are often promoted through activities designed to expand network capacity and digital services in under-developed countries. Rather than directly through public policy, the private sector thusly strengthens a state's ability to perform the functions of cybersecurity by setting certain technical standards while building digital infrastructures. In this sense, projects like Huawei's 5G rollout or Microsoft's push for cloud computing represent private sector capacity building programmes with their own longer-term priorities, eventually obtaining commercial gain.

Research questions

Through the development of a case study on regional cyber policy-development in the Southern Africa Development Community, the paper examines the governance of cyberspace in a sub-regional African organisation as shaped by capacity building activities led by state and non-state actors.

The main question that this study seeks to answer is why have cyber capacity building processes failed to achieve the level of harmonisation evoked in protocols and declarations? In order to answer to the primary question, the study seeks to answer to the following secondary questions:

1. Why are regional cyber policies, protocols and declarations not always implemented at a national level?
2. What is the state of cybersecurity legislation and policy in SADC?
3. What are the drivers (national and international) of the development of cyber-policy and regulatory frameworks at a regional and sub-regional level in Africa?

Research Methodology and Data Sources

The case study is based on primary and secondary sources of data and information. Primary data has been collected through semi-structured interviews[2] and conversations with key individuals involved in the development of the sub-regional cyber policy framework. Interviews were conducted either in person or remotely. Secondary data was collected by mapping the main cyber capacity activities undertaken at SADC level. The mapping was carried out by reviewing secondary data and information, including academic papers, reports, newspaper articles, websites and official documents related to regional cyber policy and regulatory frameworks. In addition, written records, including minutes of meetings (where available), declarations or reports from regional and sub-regional meetings and any other written documentation deemed relevant, have been analysed[3].

In addition to interviews and secondary sources, the evidence was cross referenced with information contained in the cyber capacity knowledge portal, Cybil[4]. Other databases referenced include the Cyber Policy Portal of the United Nations Institute for Disarmament Research (UNIDR) and the United Nations Conference on Trade and Development 'Global Cyberlaw Tracker'.

A conceptual framework of capacity-building as an instrument to build consensus on the governance of cyberspace is used as a lens through which to examine the evidence collected both with interviews with respondents involved in processes for the development of regional cyber policy frameworks, and via mapping of cyber capacity, policy, and legislative processes. Through the lens of the conceptual framework, triangulation of findings has enabled the analysis of the role of cyber capacity building in shaping the governance of cyberspace in SADC, and of the level of harmonisation achieved at a regional level with regards to cyber policy and legislation.

The following section is a comparative analysis of the research findings from the mapping and from the interviews. The analysis is performed vertically across the thematic areas which were used for the mapping[5]. Subsequently, research findings are discussed through the lens of the conceptual framework to answer to the research questions, and last but not least, the paper concludes with some policy implications.

Cyber capacity processes in SADC

Cyber Capacity Training

Many capacity building efforts in SADC have been directed towards strengthening institutions in regard to cybersecurity through training programs and workshops. The Council of Europe through the

[2] Three government officials (from South Africa, Mozambique, and Mauritius), a representative from an industry organisation of mobile operators, and a representative from a CSO/academia were interviewed. In total, nineteen people were invited to contribute to this study.

[3] The mapping is based on an analysis of indicators relevant to cyber policy making. These indicators include: Cyber Maturity Model (CMM) assessments, policy and strategy, legal framework, CSERT/CIRT, institutional arrangement for governing cybersecurity, multilateral agreements, ratification of the malabo convention, ratification of the Budapest convention.

[4] CyBil is a web-portal managed by the Global Forum on Cyber Expertise in collaboration with partners such as the Global Cyber Security Capacity Centre, FIRST, and the Diplo Foundation, and has catalogued capacity building initiatives and projects globally.

[5] A table with the mapping is available at the following web-link:
https://docs.google.com/spreadsheets/d/1QFvG0Saqgdvvl__yWlx54_krU-roRqfWcixuhk8-GLU/edit?usp=sharing.

Global Action on Cybercrime (GLACY and its extension GLACY+) has conducted workshops on cybercrime and cyber policy for Mauritius, South Africa, Madagascar, Namibia, Tanzania, and Zambia and has been ongoing since 2013[6] (CoE, 2019a). Beyond their aforementioned technical support, the ITU has operated cybercrime workshops in Comoros (ITU, 2014) and Malawi (Jimu, 2018), and conducted 'Stakeholder Consultation and Awareness Building' in Botswana, Eswatini, Malawi, Tanzania, and Zambia (Cybil, 2019). In a separate initiative, the United Nations Office on Drugs and Crime (UNODC) provided capacity building and mentoring to Mozambique and Tanzania in 2018 (Cybil, 2019). Another project, Cyber Resilience for Development (Cyber4Dev, 2019), funded by the EU and delivered by Northern Ireland Cooperation Overseas (NI-CO), was launched in Botswana and Mauritius in 2018 and aims to increase cyber resilience while promoting multi-stakeholder approaches to the governance of cyberspace (GFCE, 2019a).

While multilateral organisations and partnerships between several states or coalitions maintained a considerable presence, individual nations also frequently initiated or led capacity building projects. The Japan International Cooperation Agency have led cybercrime training courses in Botswana and Seychelles since 2015 (JICA, 2019) (Cybil, 2019), while the US Department of State, in collaboration with AUC & ECOWAS, conducted their own cybercrime workshops for Angola, Mauritius, and Mozambique in 2015, for example (U.S State Department, 2015). Meanwhile, the Norwegian Institute of International Affairs has been providing guidance on private sector and international cooperation on capacity building for Tanzania since 2016 (NUPI, 2018), while the Norwegian Ministry of Foreign Affairs has funded the forthcoming Cybersecurity Capacity Centre for Southern Africa (C3SA) opening in South Africa in 2020 (Cybil, 2019). The United Kingdom has been a particularly active donor, funding numerous capacity building projects. The 'Cyber Investigation Skills Training for Law Enforcement', in cooperation with Interpol and Singapore, was conducted in Botswana, Eswatini, Lesotho, Madagascar, Malawi, Mozambique, Namibia, Seychelles, Zambia and Zimbabwe in 2013-2014 (INTERPOL, 2019) (Cybil, 2019). The CTO also provided support on plans and approaches to Critical Information Infrastructure Protection (CIIP) for some Commonwealth nations in SADC since 2015 (Botswana, Eswatini, Malawi, Mozambique, Lesotho, and Tanzania) (CTO, 2015) (Cybil, 2019) and reportedly provided further advise to Mauritius, South Africa, and Botswana through the Commonwealth Africa Cyber Fellows program (Cybil, 2019). Lastly, the UK funded the Commonwealth Cybercrime Initiative (CCI) from 2013 to 2016, as a consortium of the Council of Europe, CTO, ITU, Interpol, and the Organization of American States (OAS), which was active in attempting to strengthen legal frameworks in Botswana and Tanzania (The Commonwealth, 2019). Estonia has also led cyber capacity initiatives through the e-Governance academy, which advises on cybersecurity solutions and digital transformation programmes, in Angola, Tanzania, and Mauritius (eGA, 2019a), where they also conducted a project on data architecture with the aid of the Estonian multinational, Nortal (eGA, 2019b).

Private sector involvement

Nortal is only one of several private firms working on capacity building projects in SADC. However, unlike most initiatives launched by governments and CSOs, private sector capacity building is often oriented towards the enablement of certain technologies. Infrastructure rollout represents a

[6] GLACY activities from 2013-2016 are available to view with authorised access at (CoE, 2019b) or publicly at (Cybil, 2019).

significant form of network capacity building undertaken by the private sector, including considerable investments by the likes of Google and Facebook in undersea cables (Fitzgerald, 2019) (Lardinois, 2019) and other Internet enabling projects[7], but has also become increasingly apparent through an emphasis on 5G. Following a SADC ICT sub-committee meeting in 2018 (SADC, 2018) (GSMA, SADC ICT Sub-Committee commits to facilitating 5G Trials in SADC, 2018a), the technology has been launched in South Africa by Huawei and Rain (de Villiers, 2019) and in Lesotho by Vodacom (News24, 2018) while contracts for 5G partnerships are reportedly being sought across Africa by Huawei, Vodacom, Ericsson and ZTE (Nti Osei, 2019) (King, 2019). Accompanying these efforts, a number of private sector firms have released guides and frameworks for 5G network security (e.g. (Huawei, 2015) (Ericsson, 2018) (ZTE, 2019)), and capacity building efforts are often focused around similarly nascent technological investments. Microsoft for example, which recently became the first major cloud provider in Africa (Binder, 2019), runs a number of workshops, employment opportunities and policy guides through its Microsoft4Africa project (Microsoft4Africa, 2019), but has predictably emphasised cloud computing through its Cloud for Global Good policy agenda (Microsoft, 2019), along with Artificial Intelligence (Microsoft, 2018). GSMA, a major trade industry organisation that works with mobile operators across the region similarly organises cybersecurity capacity in terms of use empowerment, through capacity building courses (GSMA, 2019a) and reports on security for Mobile Money (GSMA, 2018b), the Internet of Things (IoT) (GSMA, 2019b) and 5G for Africa (GSMA, 2019c).

Not unlike the ITU, GSMA also runs a number of working groups (GSMA, 2019d) with both industry representatives and regulators to encourage certain technical and non-technical business practices, in part in the hopes of influencing policy (interview with an industry representative). Despite the very limited number of public private partnerships on cybersecurity in SADC[8], the private sector appears to engage with officials and regulators relatively often. As a priority for service providers is to limit service restrictions, recent Vodafone Sustainable Business Reports (Vodafone, 2018) (Vodafone, 2019) outline the importance of a dialogue with ministers regarding the enablement of their mobile networks, and the encouragement of an auspicious regulatory framework. However, interviews also describe how mobile service providers and government priorities have collided in SADC on matters of regulation, monitoring and cost. Yet In some nations, private firms have taken a particularly active role, as in Angola, where ZTE has purportedly aided military telecommunications (Hsueh & Nelson, 2013), or in Zambia, where Huawei stands accused of aiding the government in surveillance and political suppression through the building of certain cybersecurity capacities (Dahir, Chinese firms are driving the rise of AI surveillance across Africa, 2019) (Parkinson, Bariyo, & Chin, 2019).

Cybersecurity Maturity Models

The capacity of states in the field of cyber security is often measured along the criteria of legal, regulatory and technical frameworks and institutions (Homburger, 2019). Other criteria used to measure the cyber capacity of states are having in place instruments for policy coordination, engaging

[7] Google's 'project Loon' (Loon, 2019) or Facebook's 'Free Basics' (Facebook Connectivity, 2019), for example.

[8] A notable exception is Serianu, a pan-African consulting firm conducting assessments, auditing and training, while partnering with the Mauritius government on Cybersecurity.

in domestic capacity building such as training the workforce and leadership and creating effective cooperative frameworks and networks (Homburger, 2019).

In SADC, while there have been previous efforts, such as the ITU Computer Incident Response Teams (CIRT) readiness assessments of 2014 (ITU, 2019a) or legislative reviews (e.g.(CoE, 2015a)), more comprehensive approaches to assessing cyber capacity and needs have recently emerged. One of them, the Cybersecurity Capacity Maturity Model for Nations (CMM), as developed by the Global Cyber Security Capacity Centre (GCSCC) in 2016, is an internationally recognised assessment model that aims to holistically understand and contextualise national cybersecurity capacity in order to promote an innovative, safe and inclusive cyberspace (GCSCC, 2017). Cybersecurity Maturity Models provide a framework for measuring the maturity of a national cybersecurity program and guidance on how to reach the next stage. At the SADC level, both the Capacity Maturity Model for Nations (CMM), and the Potomac Cyber Readiness Index have been deployed.

The CMM has been conducted in ten of the sixteen SADC states, by the GCSCC and ITU in Madagascar and by the Commonwealth Telecommunications Organisation (CTO) in Eswatini, Malawi, Mozambique and Tanzania in 2016, and by the World Bank in Zambia, Botswana, Lesotho, Mauritius, and Namibia in 2017-2019, often in collaboration with the GCSCC or ITU[9] (GCSCC, 2019). The CMM is oriented towards subsequent efforts of cybersecurity initiatives by the European Union and the United Nations, like the creation of a National Cybersecurity Strategy (NCS).

Cyber policy and strategy

A number of capacity building initiatives in SADC have been specifically directed towards the National Cybersecurity Strategy (NCS) process. While the United Nations Development Programme (UNDP) and the World Bank have facilitated the creation of national ICT policies in several SADC nations at the beginning of the 21st century (DP/2001/CRP.8, 2001) (Trucano, 2016), the ICT policies that emerged (e.g. Zambia[10], Madagascar[11], Tanzania[12], Lesotho[13], Seychelles[14]) generally contain outdated language or minimal references to cybersecurity, making them ill-equipped in a contemporary context. Conversely, a National Cybersecurity Strategy (NCS), is defined by the ITU and European Union Agency For Cybersecurity (ENISA) as, "a plan of actions designed to improve the security and resilience of national infrastructures and services" and a, "high-level top-down approach to cybersecurity that establishes a range of national objectives and priorities that should be achieved in a specific timeframe" (ENISA, 2016). Following a CMM assessment, CTO collaborations have supported the drafting of an NCS in Botswana, Malawi, and Mozambique, while the ITU has supported NCS drafts or assisted with formulation of policy in Seychelles, Tanzania, Mozambique, Eswatini and Zambia and strategies have been in place in Mauritius and South Africa for more than five years (ITU, 2019b) (Cybil, 2019). However, despite these efforts, Seychelles, Tanzania, Eswatini, Zambia, and Mozambique have

[9] According to the GCSCC, the Madagascar country report (Ignatuschtschenko & Roberts, 2016) is currently the only SADC CMM assessment publicly available.

[10] National Information Communication Technology Policy, adopted 2007 (Zambia National ICT Policy, 2006).

[11] Madagascar ICT National Policy for Development, never adopted, not publicly available (Isaacs, 2007).

[12] Tanzania National ICT Policy of 2003 (Tanzania Ministry of Transport, 2003) was updated in 2016 (Ministry of Works, Transport, and Communication, 2016)

[13] ICT Policy For Lesotho, in place since 2005 (Government of Lesotho, 2018)

[14] National ICT Policy for Seychelles, adopted 2007 and still in place (NICP, 2007).

either not completed or not ratified their respective strategies, with the remaining member states lacking one entirely. In addition to the United Nations NCS guidelines, Microsoft has published and encouraged their own framework for the development of a national strategy on cybersecurity (Goodwin & Nicholas, 2013).

Cybersecurity legislation

Supporting cybersecurity legislation processes represent another aim of certain capacity building projects in SADC. UNECA provided assistance in the formulation of legal frameworks for Cybersecurity in 2015 to Seychelles, Mozambique and Tanzania, while the UK has funded legislative reviews in Namibia and Botswana (Cybil, 2019). The most significant initiative however was the ITU regional project on the 'Support for harmonization of the ICT Policies in Sub-Saharan Africa' (HIPSSA), funded by the European Union[15]. Active from 2008 to 2013, the initiative resulted in a Draft SADC Model Law on 'Computer Crime and Cybercrime' (ITU, 2013a), which involved ITU technical assistance in Eswatini, Lesotho, Namibia, Seychelles, Tanzania, Zambia and Zimbabwe (ITU, 2013b). The HIPSSA model law was clearly influential in bringing forth some legislation, such as the Tanzanian Computer Crime and Cybercrime Bill of 2013 and the Namibia Cybercrime Bill of 2013, as well as provisions to the Mauritius Computer Misuse and Cybercrime Act of 2002 (Jamil, 2014). However, beyond this its influence appears to be limited. Moreover, the project has been criticised by the Council of Europe for poor coordination and unclear or vague language on definitions and criminal offenses (Jamil, 2014).

More recently, cybercrime legislation has faced significant backlash from civil society and human rights organisations in a majority of SADC countries, including Angola[16], Botswana[17], Democratic Republic of the Congo[18], Malawi[19], Namibia[20], South Africa[21], Zambia[22] and Zimbabwe[23]. Amongst these developments are reports of mass surveillance in Botswana (Botswana Guardian, 2015) (Freedom House, 2018b), Namibia (Links, 2018) (Mare, 2019), Angola (Fonseca, 2017) and Mozambique (Tsandzana, 2016) censoring of social media in Zimbabwe (BBC, 2019) and Zambia (Freedom House, 2018d) and extended Internet shutdowns in the Democratic Republic of the Congo (Dahir, 2018) (Burke, 2019) in the guise of cybersecurity. Indeed, according to a recent report by the UN Special Rapporteur on the rights to freedom of peaceful assembly and of association, "A surge in legislation and policies aimed at combating cybercrime has also opened the door to punishing and surveilling activists and protesters in many countries around the world" (A/HRC/41/41, 2019, p. 2).

[15] The project aimed to build on previous harmonisation projects in the region, such as the 'Regional Telecommunications Restructuring Program' (RTRP) of 1994-1998 and the 'Telecoms Harmonization' project from 1998-2004 funded by USAID, as well as the Regional ICT Support Program (RICTSP) of 2006 - 2009 funded by the EU (HIPSSA Project, 2013).

[16] Article 26 of the 2010 state security law and new Press laws part of the Social Communication Legislative Package (Freedom House, 2018a)

[17] Proposed amendments to the Cyber Crime Act (Freedom House, 2018b)

[18] law No. 013/2002 governing the security of the telecommunications sector (Access Now & Rudi International, 2018) (Dahir, 2018)

[19] Electronic Transactions and Cybersecurity Act of 2016 (MISA, 2015) (Freedom House, 2018c)

[20] Electronic Transactions and Cybercrime Bill of 2017 (Links, 2018)

[21] The Cybercrimes and Cyber Security Bill, first introduced in 2015 (SAHRC, 2017) (Sutherland, 2017)

[22] Cybersecurity and Cybercrimes Bill of 2018 (Freedom House, 2018d) (Lusaka Times, 2018)

[23] Computer Crime and Cybercrime Bill of 2017 (Kenyanito & Singh Chima, 2016) (Saki, 2017)

Therefore, cybersecurity legislation aimed at the protection of users and networks from risks remains scarce in SADC, instead consisting mostly of cybercrime laws which focus on the offence and on criminalising online behaviour. Dedicated cybercrime bills have been enacted in Madagascar in 2014, Mauritius in 2003, Seychelles in 1998, Namibia in 1988, Zimbabwe in 2004 and 2019, and South Africa and Zambia in 2004 and 2018 (UNIDR, 2019) (UNCTAD, 2019), though the Computer Misuse Act in Namibia is inadequate for the current technological landscape (CoE, 2015b). Draft bills on cybercrime, have also been introduced in Botswana in 2018, Eswatini in 2014, and Namibia, Lesotho and Seychelles in 2013, and South Africa, Malawi, Mauritius, Zambia, and Zimbabwe have slightly broader cybersecurity laws (UNCTAD, 2019) (UNIDR, 2019). Angola has also enacted a cybersecurity law on the protection of information networks in 2017 and Mauritius and South Africa have enacted new laws on data protection in 2017 and 2013 respectively. Comoros and The Democratic Republic of the Congo meanwhile are entirely lacking in both ratified and proposed cybersecurity legislation.

Institutional arrangements

Institutional arrangements responsible for creating, governing and managing cybersecurity capacities vary from state to state in SADC. All members have a department or ministry related to communications or ICT, but few have an institution dedicated to cybersecurity; only Mauritius, with its IT Security Unit and National Computer Board, Zimbabwe, with its Department of ICT Systems Security, as well as South Africa, with its National Cybersecurity Advisory Council and Cybersecurity Hub were found. Mauritius and Zambia both have an 'ICT authority' responsible for overseeing cybersecurity initiatives like the National Computer Board and zm-CIRT, and in the case of Botswana, Tanzania and Malawi, cybersecurity capacity, including the planned and operational CIRTs, often falls under the jurisdiction of the communications regulatory authorities, BOCRA, TCRA, and MACRA, respectively. In Seychelles, an IT division under the president is responsible for cybersecurity, while some ICT ministries have a designated chair, like the minister of cyber security in the Ministry of Information Communication Technology, Postal and Courier Services in Zimbabwe. However, in Namibia, Mozambique, DRC, Angola, Comoros, Eswatini and Lesotho, responsibility for cybersecurity in Government is unclear.

Incident response

Technical cybersecurity capacity in SADC has also been developed through the support for the creation of cybersecurity response teams (generally referred to as a CSIRT, CIRT, or CERT). These teams are tasked with preventing, analysing, and responding to cyber incidents, among other services and functions aimed at creating a more secure cyberspace[24]. National CSIRTs have been set up by the ITU in Zambia and Tanzania, and are also in place and operational in South Africa and Mauritius (ITU, 2019a). Phase 1 of operations are reportedly underway in Botswana following a CTO policy collaboration (BOCRA, 2019) and plans have been announced in Angola (ANGOP, 2019) and Malawi (MACRA, 2019), though signs of implementation are limited. Best-practices and standards for technical cybersecurity response are created by the Forum of Incident Response and Security Teams (FIRST), who also provided technical capacity training for incident response in Botswana under EU funds (Cybil, 2019). Beyond national CSIRTs, incident response is reportedly provided *ad hoc* by

[24] A comprehensive review of these services and functions can be found in the CSIRT Services Framework, as outlined by the Forum of Incident Response and Security Teams (FIRST, 2019).

telecommunications providers in Madagascar (Ignatuschtschenko & Roberts, 2016), while South Africa has internationally recognised sectoral CSIRTs, led by the financial sector (South African Banking Risk Information Centre SABRIC). Both South Africa and Mozambique[25] have CSIRTs run by academia (SANReN CSIRT, UCT-CIRT and MoRENET). Six SADC countries (i.e. Comoros, DRC, Eswatini, Lesotho, Seychelles, and Zimbabwe) have neither implemented nor announced CSIRTs of national or sectoral capacity, although a CSIRT readiness assessment was conducted by the ITU in 2014 for DRC, Lesotho, Eswatini, and Zimbabwe (ITU, 2019a).

Regional and multilateral agreements

International treaties, conventions and agreements can improve cyber capacity through collaboration, information-sharing, and harmonisation of cybersecurity policies and frameworks. While a fair number of bilateral, cross-border agreements on cybersecurity have been introduced in SADC and the African Union at large, most remain unratified. The Budapest Convention on Cybercrime, the first international treaty of its kind, has been signed by South Africa, and ratified only by Mauritius (CoE, 2019c). The African Union Convention on Cyber Security and Personal Data Protection, also referred to as the Malabo convention, has been signed by Comoros, Mozambique and Zambia, but only ratified by Namibia and Mauritius (African Union, 2019). Smaller or regional agreements are also in force in Malawi, which reportedly has a 'Memorandum of Understanding' with Uganda on Cybersecurity, policy, and capacity building (Rwakenya, 2017), and in Seychelles, which reportedly has multilateral cybersecurity agreements with India and Cyprus (Standard, 2018) (Laurence, 2018), but the regional impact of these are unclear. Mauritius and Tanzania are also members of the Global Forum of Cyber Expertise (GFCE, 2019b) while only Botswana, South Africa and Mauritius are members of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (GIP Digital Watch Observatory, 2019a). Although all the remaining SADC members are represented in the newly established Open-Ended Working Group (A/RES/73/27, 2018), which focuses on in the implementation of the 2015 UN GGE recommendations (A/70/174, 2015), most SADC countries were absent from the September 2019 meeting, and only South Africa, Botswana, and Mauritius made an intervention during the meeting[26].

Cybersecurity awareness (public education or training programs)

Cybersecurity awareness and public engagement programs have also been launched with the aim of building cyber capacity. While the Global Forum on Cyber Expertise has analysed a number of international efforts and organisations focused on awareness raising (Bate, Housen-Couriel, Berenblum, & Baa, 2019), such as Alert Africa, initiatives in SADC were found to be most commonly driven by the government department or body responsible for cybersecurity. Zimbabwe's Ministry of ICT, launched an annual Cybersecurity Awareness Week (Munyoro, 2019), while South Africa's Cybersecurity HUB has campaigns on public awareness and safety, and Mauritius' National Computer Board provides cyber capacity and safety training for people and businesses (National Computer Board, 2019). Academic institutions also contribute to public awareness and capacity, for example

[25] MZ-CIRT in Mozambique has a web presence, but is neither recognised by the ITU, nor a member of any international CIRT networks, and it is also not affiliated with the government, its activity or status could therefore not be verified.
[26] Full meeting reports available at (GIP Digital Watch Observatory, 2019b)

through the MoRENET network in Mozambique, or through cybersecurity competitions at the Namibia University of Science and Technology (NUST, 2016).

Discussion

Through the analysis of the main cyber capacity processes which are shaping the governance of cyberspace in SADC, this paper has sought to answer to the main question on why cyber capacity building processes failed to achieve the level of harmonisation evoked in protocols and declarations. The main following reasons have emerged from the analysis:

1. *Uneven levels of ICT development*

One of the most obvious reasons for lack of harmonisation of cyber policy and legislation at SADC level is that substantial differences in terms of ICT development persist across SADC countries (see Figure 1 below), which may result in differences in terms of how cybersecurity is prioritised. Although a number of cyber capacity building programmes may assume a certain level of ICT development, the sub-regional average of Internet penetration is of only 26% (with a range of between 4,7% and 56,5%) (ITU, 2017), and both demand and supply side challenges persist (Mothobi, Chair, & Rademan, 2017). Affordability is cited as a key barrier to Internet uptake in the region, with other user issues such as a lack of digital literacy and a lack of relevant content impacting uptake and experience (Research ICT Africa, 2017).

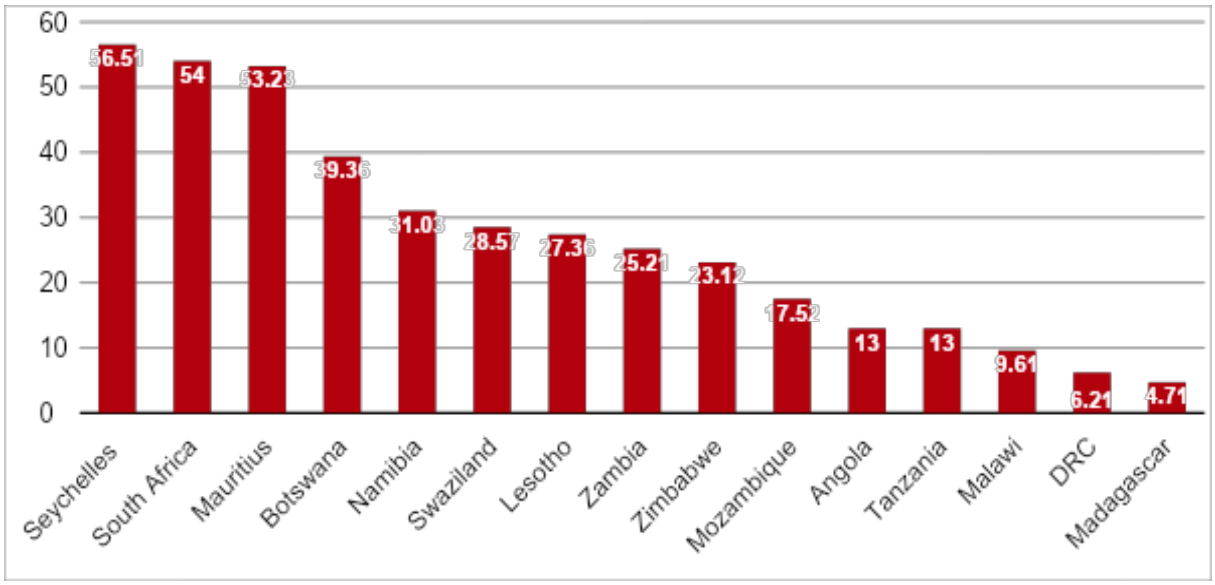

Figure 1: Percentage of individuals using the Internet in SADC countries

Source: ITU statistics, 2017

Limited access, low uptake and uneven digital infrastructure does not mean that SADC faces less cyber risk than other regions. While the critical mass necessary to enjoy the network benefits of the Internet is estimated to be a penetration of 20% (Gillwald & Mothobi, 2019), analysts have suggested that the threshold for the generation of significant hacking activities lies at 10 to 15% (Kshetri, 2013).

2. *Several competing agendas, with resulting competing priorities*

The norms, standards, and best practices that are encouraged through the wealth of capacity building initiatives undertaken at SADC level—though global in ambition—are oft not built on regionally held or national priorities. Overall, these capacity building activities appear fragmented and underpinned by different objectives and priorities. Generally, they emerge out of small groups of experts, or 'epistemic communities' (Haas, 1992), through networks of elite organisations and prestigious conferences (Shires, 2018) (Tanczer, Brass, & Carr, 2018) that largely represent the agendas of influential donors and political coalitions. Given this, the priorities of under-resourced regions like Sub-Saharan Africa are less likely to be considered, or acted upon exclusively. Indeed, Africa can be described as 'a resilient but marginal player' (Gruzd, Mutangadura, & de Carvalho, 2019, p. 2) in the global dialogue for the governance of cyberspace. Yet at regional, sub-regional and national levels, SADC has its own political economy and Internet ecosystems, and therefore faces a distinct set of challenges in securing its cyberspace. Cyber-threat is compounded by the lack of digital skills and public awareness on cybersecurity. The Research ICT Africa, nationally representative 'After Access' surveys found that many Internet users are novices with little awareness of mobile security risks and with little or no protection, as transactions are often computed in countries without or with nascent cybersecurity and data protection legislations (Research ICT Africa, 2017). The region also lacks technical capacity with only a few technical cybersecurity teams ready to respond to threats. This has resulted in Africa being a continent with one of the highest rates of cybercrime affecting the strategic, economic and social growth development of the region (Oladipo, 2015) (Serianu, 2016).

3. *4th Industrial Revolution and the private sector priorities*

The incentive of the private sector in cybersecurity, mainly motivated by the economic gains, is characterised by a paradigm of opportunities and risks rather than promoting a user's rights-based model for the governance of the Internet. These efforts revolve around protecting and expanding investments — without securing networks or IT services, their business is at risk, and enabling new "4th Industrial Revolution" technologies like 5G, IoT, Cloud Computing, or AI, instead of representing significant opportunities for profit, may place them under government restrictions or rules. In this sense, capacity building projects led by the private sector are generally bound by specific priorities linked to the technology or service that they want to promote, and in turn they are able to shape the governance of cyberspace by suggesting policy and regulatory framework that facilitate investment and use of those technologies. Facebook exemplifies this, through the company's primary security research objectives of, "protecting accounts from phishing and malware, as well as developing long-term solutions to ensure that Facebook remains one of the best mediums for communicating personal information to your friends and family" (Facebook Research, 2019).

4. *Uneven outputs in terms of NCS, cyber policy, legislation, and institutional arrangements*

A number of capacity building activities in SADC have taken the form of technical support, training programs and workshops with the aim of strengthening institutions, while other initiatives aimed to increase cyber resilience and promoting multi-stakeholder approaches to the governance of cyberspace. However, despite a plethora of cyber capacity building initiatives in SADC, their outputs in terms of strengthening institutions, or supporting countries in developing National Cyber Strategies or cyber policy and regulation has been uneven. By the end of 2019, only three countries have a

national cyber policy or strategy in place (i.e. Botswana, Mauritius, and South Africa). Malawi, Mozambique, Tanzania, and Zambia, are still at a drafting stage, while Comoros, DRC, Eswatini, and Seychelles do not have cyber policy in place. Many countries (Botswana, Eswatini, Lesotho, Namibia, Seychelles) are still at a drafting stage of their cybersecurity or crime bills. Overall, cybersecurity legislation aimed at protecting users and networks from risk is uneven in SADC. Rather, current processes aim towards cybercrime laws which focus on the offence and on criminalising online behaviour. Last but not least, only a few countries have a dedicated institution dealing with cybersecurity (Mauritius, Zimbabwe, and South Africa), raising serious concerns related to the capacity of these countries to implement and enforce cyber legislation.

4. Human rights concerns in relation to cybercrime legislation

Democratic assumptions about human rights, freedom of expression, privacy, and security that inform policies and the approach to cybersecurity advocated by the European Union and its like-minded allies may diverge from those in African countries (Gillwald, 2014). The accepted and ratified human rights framework which informs cyber-policy making to address issues such as privacy protection, free flow of information or freedom of expression (Jørgensen, 2013), is based on the Western values of mature democracies and often collides with the political economy of fragile Southern African democratic states (Khan, 2002) (Khan, 2005) as well as with their under-resourced institutional arrangements, which often lack necessary technical skills and financial resources to effectively implement reforms (Gillwald, 2005).

Although SADC countries are committed by its treaty to act in accordance with the principles of human rights, democracy and the rule of law (in addition to having human rights obligations in national constitutions, and to be bound to the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and the African Charter on Human and Peoples' Rights), the majority of countries who have cybercrime legislation in place have been highly criticized by civil society and human rights organisations for their approaches and measures to securing the Internet. In the guise of cybersecurity, a number of measures restricting human rights line have been registered: compulsory SIM cards registration, mass surveillance and warrant-less surveillance practices[27], use of spyware by government organisations, threats of expansion of the cybercrime acts to stifle freedom of expression online, conferment of powers governments to take charge of communication facilities in the interest of national security or public defence, have been reported in a number of countries. These practices are normally contrary to the values and ideology underpinning human rights and good governance frameworks promoted by cyber capacity programmes and activities.

Conclusion and policy recommendations

Assessing the appropriate role for the State in the governance of the cyberspace and the institutional arrangements that arise from it is one of the primary policy challenges facing cyber-capacity

[27] It is worthwhile in this context to consider the recent judgment on South Africa's interception legislation, *Amabhungane Centre for Investigative Journalism NPC and Another v Minister of Justice and Correctional Services and Others* [2019] ZAGPPHC 384. The court deemed certain aspects of the law as unconstitutional, because the procedural aspects described for gaining permissions in terms of the Act were generally insufficiently detailed, and failed to provide for adequate oversight of requests.

programmes in developing countries. States are critical to respond to cyber threats, and effective state-led measures can guarantee cybersecurity based on the rule of law; they can also facilitate the design and implementation of effective strategies to insure the development, implementation and enforcement of legal frameworks for a safe and secure cyberspace. Yet, a technical and normative approach to institutions, processes and rules in this area, which is outside a human rights and good governance framework, may have the unintended outcome of effectively weakening the protection of individual rights (Bau & Calandro, 2019). Although development theory is based on a commitment to freedom, equity and cooperative interdependence, a necessary part of supporting development processes must include holding States accountable to their commitment to the Universal Declaration of Human Rights as a global governance standard (Gillwald, 2014). Hence, a rights-based approach should be at the core of a safe Internet.

Cyber capacity building programmes to strengthen institutions and to improve cyber postures, compounded with cyber awareness programmes to reduce risks and harms associated with cybercrime, in SADC have resulted in uneven adoption, from national governments, of international standards for the governance of cybersecurity (including cyber strategies, policies, and legislations) and in the establishment of only a few operational Computer Emergency Response Teams (CERTs). Unclear institutional arrangements many SADC countries make them highly vulnerable to fast-changing and sophisticated cyber-attacks. Different ideologies, objectives, and priorities have informed different approaches to cyber capacity building and may result in fragmentation of approaches to the global and regional governance of cyberspace. In addition, many of these capacity building activities are a once-off exercise with no follow-up, while countries certainly need more structured and long-term programmes for their cyber posture to improve. Therefore, organisations dealing with cyber capacity should improve the coordination of their objectives and activities, to reduce fragmentation and improve impact at a national level. A good practise in this field is the Global Forum of Cyber Expertise, which aims at improving coordination between cyber capacity activities, and at acting as a clearing house between countries in need, donors, and organisations and individuals able to provide technical assistance. Other coordinating initiatives in this domain are the Forum of Incident Response and Security Teams (FIRST) which provides technical support for national CSIRTs, and the Global Cyber Security Capacity Centre which focuses on cyber maturity assessment and on academic research on cyber capacity.

Considering capacity challenges and difficulties in both developing cyber policy and regulatory frameworks, and even more, in implementing and enforcing existing laws in this domain, African policy makers should reflect on their ability to enforce new binding treaties on the governance of cyberspace currently under discussion at a UN level. Capacity building is needed indeed to observe the non-binding, and voluntary norms, principles and rules on responsive state behaviour in cyberspace agreed upon with resolution (A/70/174, 2015), and to clarify how international laws apply in cyberspace. Therefore, once again, it is recommended that policies should aim at improving coordination efforts between all stakeholders dealing with cyber capacity building, to allow existing UN resolutions to be effectively implemented. Nationally, cyber maturity assessments can identify specific points of policy intervention, and overall align the region in terms of cyber objectives, priorities, and actions.

ICT plays a crucial role in achieving the Sustainable Development Goals (SDGs), considering well known developmental aspects related to digitalisation. However, at the same time, it is necessary to not only

build a realistic understanding of how the Internet, specifically, can contribute towards the SDGs at a global, national and local scale, but also to identify how to overcome harms and respond to risks that might arise as digitalisation permeates all social and economic activities of our societies. In relation to peace, justice and strong institutions, the focus of SDG 16, the use of open data by governments offers increased transparency and empowers citizens by allowing them to make critical choices for their lives, which indirectly support economic growth. This, again, calls for a collaborative security approach that builds trust in online services, ensures that data are secure, and makes the use of networks and services reliable.

Future research

More regionally-focused research on cyber capacity is needed to assess specific points of cyber policy intervention at a national and regional level. With the establishment of a Cybersecurity Capacity Centre in Southern Africa in 2020, an initiative in collaboration between the Global Cyber Security Capacity Centre at Oxford, Research ICT Africa, the University of Cape Town, and the Norwegian Institute of International Affairs, it is expected that coordination and collaboration between cybersecurity capacity building actors will improve in SADC by providing a single entry point for cybersecurity capacity building and research activities in the region and by reducing duplication of efforts. Through the deployment of the Cyber Maturity Model for Nations, an established method to assess cybersecurity capacity at a national level, locally informed educational programme can also be developed.

References

A/53/PV.79. (1998, December 4). *United Nations General Assembly.* Retrieved from https://undocs.org/en/A/53/PV.79

A/70/174. (2015, July 22). *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.* Retrieved from United Nations General Assembly: https://dig.watch/sites/default/files/UN%20GGE%20Report%202015%20%28A-70-174%29.pdf

A/C.3/74/L.11. (2019, October 11). Retrieved from UN General Assembly: https://undocs.org/A/C.3/74/L.11

A/HRC/41/41. (2019, May 17). *Rights to freedom of peaceful assembly and of association Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association.* Retrieved from United Nations General Assembly: https://undocs.org/A/HRC/41/41

A/RES/73/27. (2018, December 5). *Developments in the field of information and telecommunications in the context of international security.* Retrieved from United Nations General Assembly: https://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/73/27

Access Now & Rudi International. (2018). *Joint submission to the United Nations Human Rights Council, for the 33rd Session of the Universal Periodic Review for Democratic Republic of Congo.* Retrieved from Access Now: https://www.accessnow.org/cms/assets/uploads/2018/10/DRC-digital-rights.pdf

African Union. (2014). *African Union Convention on Cyber Security and Data Protection.* Retrieved from https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

African Union. (2019, June). *List of Countries Which Have Signed, Ratified/Acceded to the African Union Convention on Cybercrime and Personal Data Protection.* Retrieved from African

Union: https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf

ANGOP. (2019, July 26). *State to spend USD 11 million / year on cyber security*. Retrieved from Agencia Angola Press: http://www.angop.ao/angola/en_us/noticias/economia/2019/6/30/State-spend-USD-million-year-cyber-security,2283adbf-4b93-4344-96c3-e3cb3148c144.html

Arimatsu, L. (2012). A Treaty for Governing Cyber-Weapons: Potential Benefi ts and Practical Limitations. *2012 4th International Conference on Cyber Conflict* (pp. 91-109). Talinn: NATO CCD COE Publications.

Ariu, D., Didaci, L., Fumera, G., Giacinto, G., Roli, F., Frumento, E., & Freschi, F. (2016). A (Cyber)ROAD to the Future: A Methodology for Building Cybersecurity Research Roadmaps. In B. Akhgar, & B. Brewster, *Combatting Cybercrime and Cyberterrorism* (pp. 55-77). Switzerland: Springer.

Bate, L., Housen-Couriel, D., Berenblum, T., & Baa, M. (2019, March 21). *White Paper: Task Force on Cyber Security Awareness.* Retrieved from Global Forum on Cyber Expertise: https://csrcl.huji.ac.il/sites/default/files/csrcl/files/gfce_wg_d_white_paper_task_force_cyber_awareness.pdf

Bau, V., & Calandro, E. (2019). The Experience of Online Freedom among Internet Users in Africa. *Information, Communication and Society (Under Review)*.

BBC. (2019, January 18). *Zimbabwe blocks Facebook, WhatsApp and Twitter amid crackdown*. Retrieved from BBC News: https://www.bbc.com/news/world-africa-46917259

Binder, M. (2019, March 7). *Microsoft officially becomes first major cloud provider in Africa.* Retrieved from Mashable: https://mashable.com/article/microsoft-south-africa-azure-cloud-data-center/

BOCRA. (2019). *Botswana Communications Regulatory Authority*. Retrieved from BW-CIRT: https://www.bocra.org.bw/bw-cirt

Botswana Guardian. (2015, February 23). *DIS launches massive surveillance programme.* Retrieved from Botswana Guardian: http://www.botswanaguardian.co.bw/news/item/1284-dis-launches-massive-surveillance-programme.html

Breuer, H., & Webel, S. (2019). *Time for Action: Building a Consensus for Cybersecurity. The Charter of Trust: Ten steps to a more secure world.* Retrieved from Siements: https://new.siemens.com/global/en/company/stories/research-technologies/cybersecurity/cybersecurity-charter-of-trust.html

BRICS. (2014, July 15). *Fortaleza Declaration.* Retrieved from Sixth BRICS Summit: https://www.gcis.gov.za/content/newsroom/media-releases/media-statements/6th-BRICS-declaration

Burke, J. (2019, January 1). *DRC electoral fraud fears rise as internet shutdown continues*. Retrieved from The Guardian: https://www.theguardian.com/world/2019/jan/01/drc-electoral-fears-rise-as-internet-shutdown-continues

Calandro, E. (2015). Governing Regional Telecommunication Networks in a Developing Region: The SADC Case. *Unpublished PhD Thesis*. Cape Town: University of Cape Town, Graduate School of Business.

CoE. (2011). ETS 185 – Convention on Cybercrime, 23.XI.2001. Budapest: Council of Europe. Retrieved from https://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

CoE. (2015a). *Octopus Cybercrime Community: Legislative Profiles*. Retrieved from Council of Europe: https://www.coe.int/en/web/octopus/country-legislative-profile

CoE. (2015b). *Namibia: Status Regarding Budapest Convention.* Retrieved from Council of Euope: https://www.coe.int/en/web/octopus/country-wiki/-/asset_publisher/hFPA5fbKjyCJ/content/namibia/pop_up?inheritRedirect=false

CoE. (2019a). *Global Action on Cybercrime Extended (GLACY)+*. Retrieved from Council of Europe: https://www.coe.int/en/web/cybercrime/glacyplus

CoE. (2019b). *Glacy.* Retrieved from Council of Euope: http://www.coe.int/en/web/cybercrime-staging/glacy

CoE. (2019c, November). *Chart of signatures and ratifications of Treaty 185: Convention on Cybercrime.* Retrieved from Council of Europe: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures

CTO. (2015). *Southern African Regional CIIP Workshop*. Retrieved from https://www.cto.int/strategic-goals/cybersecurity/ciip-workshops/southern-african-regional-ciip-workshop/

Cyber4Dev. (2019). *Cyber Resilience for Development is a European Union*. Retrieved from https://cyber4dev.eu/

Cybil. (2019). Retrieved from Cyblil Portal: https://cybilportal.org/

Dahir. (2018, January 24). *There's a decades-old law threatening digital freedom in DR Congo*. Retrieved from Quartz Africa: https://qz.com/africa/1187727/the-dr-congo-is-using-a-decades-old-law-to-shut-down-the-internet/

Dahir. (2019, September 18). *Chinese firms are driving the rise of AI surveillance across Africa*. Retrieved from Quarz Africa: https://qz.com/africa/1711109/chinas-huawei-is-driving-ai-surveillance-tools-in-africa/

de Villiers, J. (2019, September 18). *South Africa's first 5G network is now live in parts of Johannesburg and Tshwane – here's what you'll pay*. Retrieved from Business Insider: https://www.businessinsider.co.za/south-africa-first-5g-cellular-network-johannesburg-tshwane-rain-cellular-network-2019-9

DP/2001/CRP.8. (2001, June 8). *Role of UNDP in information and communication technology for development.* Retrieved from United Nations Development Programme: http://web.undp.org/execbrd/pdf/DP2001CRP8.PDF

E/2002/58. (2002, May 14). *United Nations system support for capacitybuilding.* Retrieved from United Nations: https://unispal.un.org/DPA/DPR/unispal.nsf/0/39CF918D783D0CE785256CCB005527CA

eGA. (2019a). *Introducing Estonian ICT solutions for delegations from developing countries*. Retrieved from e-Governance Academy: https://ega.ee/project/introducing-estonian-ict-solutions-for-delegations-from-developing-countries/

eGA. (2019b). *Data Sharing Policy and Data Architecture for Mauritius*. Retrieved from e-Governance Academy: https://ega.ee/project/data-sharing-policy-and-data-architecture-for-mauritius/

ENISA. (2016). *National Cyber Security Strategies.* Retrieved from European Union Agency for Cybersecurity: https://resilience.enisa.europa.eu/enisas-ncss-project

Ericsson. (2018). *A guide to 5G network security.* Retrieved from Ericsson: https://www.ericsson.com/en/security/a-guide-to-5g-network-security

Facebook Connectivity. (2019). Retrieved from https://connectivity.fb.com/free-basics/

Facebook Research. (2019). *Security & Privacy: Keeping the Facebook community safe and secure.* Retrieved from Facebook Research: https://research.fb.com/category/security-and-privacy/

FIRST. (2019, June). *Computer Security Incident Response Team (CSIRT) Services Framework Version 2.0 (Review Release).* Retrieved from FIRST: https://www.first.org/education/FIRST_CSIRT_Services_Framework_v2.0.pdf

Fitzgerald, D. (2019, April 7). *Facebook Looks to Build Underwater Ring Around Africa*. Retrieved from The Wall Street Journal: https://www.wsj.com/articles/facebook-looks-to-build-underwater-ring-around-africa-11554649200

Fonseca, J. B. (2017). The Authoritarian Government of Angola learning High-Tech Surveillance. *Surveillance & Society, 15*(3), 371-380.
Freedom House. (2018a). *Freedom of the Net: 'Angola' Country Report.* Retrieved from Freedom House: https://freedomhouse.org/report/freedom-net/2018/angola
Freedom House. (2018b). *Freedom In the World: 'Botswana' Country Report.* Retrieved from Freedom House: https://freedomhouse.org/report/freedom-world/2018/botswana
Freedom House. (2018c). *Freedom of the Net: 'Malawi' Country Report.* Retrieved from Freedom House: https://freedomhouse.org/report/freedom-net/2018/malawi
Freedom House. (2018d). *Freedom House*. Retrieved from Freedom of the Net: 'Zambia' Country Report: https://freedomhouse.org/report/freedom-net/2018/zambia
GCSCC. (2017, February 9). *Cybersecurity Capacity Maturity Model for Nations (CMM).* Retrieved from Global Cyber Security Capacity Centre: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CMM%20revised%20edition_09022017_1.pdf
GCSCC. (2019). *CMM Assessments Around the World.* Retrieved from Glocal Cyber Security Capacity Centre: https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cmm-assessments-around-world
GFCE. (2019a). *Cyber4dev*. Retrieved from Global Forum on Cyber Expertise: https://www.thegfce.com/initiatives/cyber4dev
GFCE. (2019b). *Members and Partners*. Retrieved from Global Forum on Cyber Expertise: https://www.thegfce.com/members-and-partners/members
Gillwald, A. (2005). *Towards an African e-Index: Household and individual ICT Access and Usage across 10 African countries.* Johannesburg: The Link Centre.
Gillwald, A. (2014). *Comments for Stockholm Internet Forum (SIF14).* Retrieved from Research ICT Africa: https://researchictafrica.net/2015/05/29/comments-for-stockholm-internet-forum-sif14-by-alison-gillwald/
Gillwald, A., & Mothobi, O. (2019). *After Access 2018: A Demand-Side View of Mobile Internet From 10 African Countries.* Research ICT Africa.
GIP Digital Watch Observatory. (2019a). *UN GGE and OEWG*. Retrieved from Geneva Internet Platform. Diplo Foundation: https://dig.watch/processes/un-gge
GIP Digital Watch Observatory. (2019b). *Open-Ended Working Group (OEWG) - First substantive session.* Retrieved from Geneva Internet Platform: Digital Watch Observatory: https://dig.watch/events/open-ended-working-group-oewg-first-substantive-session#reports
Gold, J. (2019, May 16). *Two Incompatible Approaches to Governing Cyberspace Hinder Global Consensus*. Retrieved from Leiden Security and Global Affairs Blog: https://leidensecurityandglobalaffairs.nl/articles/two-incompatible-approaches-to-governing-cyberspace-hinder-global-consensus
Goodwin, C. F., & Nicholas, J. P. (2013, October). *Developing a National Strategy for Cybersecurity Foundations For Security, Growth, and Innovation.* Retrieved from Microsoft: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/REVoNi
Government of Lesotho. (2018). *Lesotho ICT Policy.* Retrieved from Government of Lesotho Official Website for The Kingdom of Lesotho: https://www.gov.ls/documents/lesotho-ict-policy/
Gruzd, S., Mutangadura, C., & de Carvalho, G. (2019). *Africa Report 18: At the table or on the menu? Africa's agency and the global order.* Institute for Security Studies.
GSMA. (2018a, July 21). *SADC ICT Sub-Committee commits to facilitating 5G Trials in SADC*. Retrieved from GSMA: https://www.gsma.com/subsaharanafrica/sadc-ict-sub-committee-commits-to-facilitating-5g-trials-in-sadc
GSMA. (2018b, June 29). *MM App Security Best Practices.* Retrieved from GSMA: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2018/08/Mobile-money-app-security-best-practices.pdf
GSMA. (2019a). Retrieved from GSMA Capacity Building: https://www.gsmatraining.com/courses/

GSMA. (2019b). *GSMA IoT Security Guidelines and Assessment.* Retrieved from GSMA: https://www.gsma.com/iot/iot-security/iot-security-guidelines/
GSMA. (2019c). *5G in Sub-Saharan Africa: laying the foundations.* Retrieved from GSMA: https://www.gsmaintelligence.com/research/?file=7d4569ab4c1f69b82e9ad8f179ba92ef&download
GSMA. (2019d). *Fraud and Security Group.* Retrieved from GSMA: https://www.gsma.com/aboutus/workinggroups/fraud-security-group
Haas, P. (1992). Introduction: Epistemic Communities and International Policy Coordination. *International Organization, 46*(1), 1-35.
Hameiri, S. (2009). Capacity and its Fallacies: International State Building as State Transformation. *Millennium: Journal of International Studies, 38*(1), 55-81.
Homburger, Z. (2019). The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace. *Global Society*, 224-242 DOI: 10.1080/13600826.2019.1569502.
Hsueh, R., & Nelson, M. B. (2013). Who Wins? China Wires Africa: The Cases of Angola and Nigeria. *NYU/Giessen Development Finance Conference.* New York City: New York University School of Law.
Huawei. (2015). *5G Security: Forward Thinking Huawei White Paper.* Retrieved from Huawei: https://www.huawei.com/minisite/5g/img/5G_Security_Whitepaper_en.pdf
Hurwitz, R. (2014, Vol. 36, No. 5). The Play of States: Norms and Security in Cyberspace. *American Foreign Policy Interests*.
Ignatuschtschenko, E., & Roberts, T. (2016, November 22). *Cybersecurity Capacity Review of the Republic of Madagascar.* Retrieved from Global Cyber Security Capacity Centre: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/cmm_rapport_final_cybersecurite_madagascar.pdf
INTERPOL. (2019). *Cybercrime training for police*. Retrieved from Interpol: https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-training-for-police
Isaacs, S. (2007, April). *ICT in Education in Madagascar .* Retrieved from World Bank Info Dev : https://www.infodev.org/infodev-files/resource/InfodevDocuments_413.pdf
ITU. (2013a). *Computer Crime and Cybercrime: Southern African Development Community (SADC) Model Law.* Retrieved from HIPSSA: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/SADC%20Model%20Law%20Cybercrime.pdf
ITU. (2013b). *Key Performance Indicator (KPI) - In-Country Technical Assistance. HIPSSA.* Retrieved from International Telecommunications Union: https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/In-country%20support%20documents/HIPSSA_KPI_In-country_Technical_Assistance_9Oct2013.pdf
ITU. (2014). *LDCs Infrastructure Protection Program: Comoros, 1-5 September 2014*. Retrieved from International Telecommunications Union: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/LDC_Comoros.aspx
ITU. (2017). *Measuring the Information Society Report*. Geneva: International Telecommunications Union.
ITU. (2019a). *National CIRT*. Retrieved from International Telecommunications Union: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx
ITU. (2019b). *National Cybersecurity Strategies Repository.* Retrieved from International Telecommunications Union: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx
Jørgensen, R. F. (2013). An internet bill of rights? In I. Brown, *Research Handbook on Governance of the Internet* (pp. 353-372). Cheltenham, UK: Rdward Elgar Publishing Ltd.
Jamil, Z. (2014, December 9). *Cybercrime Model Laws Discussion paper prepared for the Cybercrime Convention Committee (T-CY).* Retrieved from Council of Europe: https://rm.coe.int/1680303ee1

JICA. (2019). *Countermeasures against Cybercrime*. Retrieved from Japan International Cooperation Agency: https://www.jica.go.jp/english/our_work/types_of_assistance/tech/acceptance/training/about/2018/sector/c8h0vm0000eqy9ys-att/1884518_e.pdf

Jimu, C. (2018, March 16). *Malawi moves to secure its cyber space*. Retrieved from MW Nation: https://mwnation.com/malawi-moves-secure-cyber-space/

Kaldor, M., Martin, M., & Selchow, S. (2007). Human Security: A New Strategic Narrative for Europe. *International Affairs, 83*(2), 273-288.

Kenyanito, E. P., & Singh Chima, R. J. (2016, December). *Room for improvement: Implementing the African Cyber Security and Data Protection Convention in Sub-Saharan Africa*. Retrieved from Access Now: https://www.accessnow.org/cms/assets/uploads/2016/12/RoomforImprovement_Africa.pdf

Khan, M. H. (2002). State Failure in Developing Countries and Strategies of Institutional Reform. In B. Tungodden, N. Stern, & I. Kolstad, *Towards Pro-Poor Policies* (pp. 165-195). Oxford: Oxford University Press.

Khan, M. H. (2005). Markets, States and Democracy: Patron-Client Networks and the Case for Demcracy in Developing Countries. In J. Faundez, *Special Issues of Democratization: on the State of Democracy.* London: SOAS, University of London.

King, J. (2019, April 10). *ZTE 5G-Oriented Core Network Evolution Solution wins 'Best Telco Digital Transformation' award at 5G MENA 2019*. Retrieved from IT Web: https://www.itweb.co.za/content/O2rQGMApjpy7d1ea

Kshetri, N. (2013). *Cybercrime and Cybersecurity in the Global South.* London: Palgrave Macmillan UK.

Kshetri, N. (2015). Cybercrime and Cybersecurity Issues in the BRICS Economies. *Journal of Global Information Technology Management, 18*(4), 245-249.

Kumar, S. (2019, October 15). *Key Takeaways From the AU GGE Consultation*. Retrieved from Global Partners Digital: https://www.gp-digital.org/key-takeaways-from-the-au-gge-consultation/

Lardinois, F. (2019, July 28). *Google Is Building a New Private Subsea Cable Between Portugal to South Africa*. Retrieved from Tech Crunch: https://techcrunch.com/2019/06/28/google-is-building-a-new-private-subsea-cable-between-portugal-and-south-africa/

Laurence, D. (2018, July 5). *Seychelles-Cyprus agreement sees ecommerce, cybersecurity as areas for cooperation*. Retrieved from Seychelles News Agency: http://www.seychellesnewsagency.com/articles/9390/Seychelles-Cyprus+agreement+sees+ecommerce%2C+cybersecurity+as+areas+for+cooperation

Links, F. (2018). *Democracy Report: Tackling Cybersecurity/Crime In Namibia - Calling For a Human Rights Respecting Framework.* Institute for Public Policy Research.

Links, F. (2018). *Tackling Cybersecurity/Cybercrime in Namibia – Calling For a Human Rights Respecting Framework.* Institute for Public Policy Research.

Loon. (2019). Retrieved from https://loon.com/

Lusaka Times. (2018, June 11). *Government Plans to Introduce Cyber Police*. Retrieved from The Lusaka Times: https://www.lusakatimes.com/2018/06/11/government-plans-to-introduce-cyber-police/

MACRA. (2019). *Malawi designs Computer Emergency Response Team*. Retrieved from Malawi Communications Regulatory Authority: https://www.macra.org.mw/malawi-designs-computer-emergency-response-team/

Mare. (2019, November). *Communication Surveillance in Namibia: An Exploratory Study*. Retrieved from The Media and Democracy Project: https://www.mediaanddemocracy.com/uploads/1/6/5/7/16577624/namibia_report_3rd_pages.pdf

Maurer, T., & Morgus, R. (2014). Tipping the Scale: An Analysis of Global Swing States in the Internet Governance Debate. *Global Commission on Internet Governance. Paper Series No. 2.* Cente For International Governance and Innovation: Chatham House.

Microsoft. (2018). *Artificial Intelligence for Africa: An Opportunity for Growth, Development, and Democratisation.* Retrieved from Microsoft: https://info.microsoft.com/rs/157-GQE-382/images/EN-CNTNT-Whitepaper-AIinAfrica2-MGC0003244.pdf

Microsoft. (2019). *Cloud For Good: A Policy Roadmap.* Retrieved from Microsoft: https://news.microsoft.com/cloudforgood/#policy-roadmap

Microsoft4Africa. (2019). *Microsoft 4 Africa.* Retrieved from Microsoft: https://www.microsoft.com/africa/4afrika/

Ministry of Works, Transport, and Communication. (2016). *Tanzania National ICT Policy.* Retrieved from https://tanzict.files.wordpress.com/2016/05/national-ict-policy-proofed-final-nic-review-2.pdf#targetText=To%20guide%20Tanzania%20in%20the,in%20service%20delivery%20to%20citizens.

MISA. (2015, November 29). *Media Institute for Southern Africa.* Retrieved from Malawi Parliament Rejects Bill to Gag Online Media: https://malawi.misa.org/2015/11/29/malawi-parliament-rejects-bill-to-gag-online-media/

Mothobi, O., Chair, C., & Rademan, B. (2017). *Policy Brief 6: SADC not bridging digital divide.* Research ICT Africa.

Muller, P. (2015). Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities, p. . Norwegian Institute of International Affairs, NUPI Report no. 3.

Munyoro, F. (2019, October 4). *Zimbabwe: Month-Long Cyber Security Awareness Crusade Begins.* Retrieved from All Africa: https://allafrica.com/stories/201910040554.html

National Computer Board. (2019). Retrieved from http://www.ncb.mu/English/Pages/default.aspx

News24. (2018, September 8). *Lesotho emerges as unlikely testbed for 5G revolution*. Retrieved from News 24: https://www.news24.com/Africa/News/lesotho-emerges-as-unlikely-testbed-for-5g-revolution-20180907-2

NICP. (2007). *National ICT Policy for Seychelles* . Retrieved from Government of Seychelles: http://www.ict.gov.sc/resources/policy.pdf

Nocetti, J. (2015). Contest and conquest: Russia and global internet governance. *International Affairs, 91*(1), 111-130.

Nti Osei, O. A. (2019, April 5). *The 5G revolution is coming to Africa*. Retrieved from The Africa Report: https://www.theafricareport.com/11461/the-5g-revolution-is-coming-to-africa/

Nunnenkamp, P. (1995). What donors mean by good governance, heroic ends, limited means, and traditional dilemmas of development cooperation. *IDS Bulletin, Vol. 26, No. 2*.

NUPI. (2018). *Cybersecurity Capacity Building 2.0 - Bridging the digital divide and strengthening sustainable development*. Retrieved from Norwegian Institute of International Affairs: https://www.nupi.no/en/About-NUPI/Projects-centers/Cybersecurity-Capacity-Building-2.0-Bridging-the-digital-divide-and-strengthening-sustainable-development

NUST. (2016). *Digital Forensics and Information Security Research Cluster (DFISRC): NUST Cyber Security Team Selection* . Retrieved from Namibia University of Science and Technology: https://www.nust.na/?q=announce/nust-cyber-security-team-selection

Oladipo, T. (2015, November 17). *Cyber-crime is Africa's 'next big threat', experts warn*. Retrieved from BBC News: https://www.bbc.com/news/world-africa-34830724

Painter, C. (2016). *International Cybersecurity Strategy: Deterring Foreign Threats and Building Global Cyber Norms.* Retrieved from U.S Department of State: https://2009-2017.state.gov/s/cyberissues/releasesandremarks/257719.htm

Panova, V. (2015). The BRICS Security Agenda and Prospects for the BRICS Ufa Summit. *International Organisations Research Journal, 10*(2), 90-104.

Parkinson, J., Bariyo, N., & Chin, J. (2019, August 15). *Huawei Technicians Helped African Governments Spy on Political Opponents*. Retrieved from The Wall Street Journal: https://www.wsj.com/articles/huawei-technicians-helped-african-governments-spy-on-political-opponents-11565793017

Pawlak, P. (2016). Capacity Building in Cyberspace as an Instrument of Foreign Policy. *Global Policy, 7*(1), 83-92.

Research ICT Africa. (2017). *After Access Surveys.* Retrieved from Research ICT Africa: https://afteraccess.net/

Rwakenya, E. (2017, February 16). *Uganda and Malawi sign pact to fight cybercrime and build capabilities*. Retrieved from SC Media: https://www.scmagazineuk.com/uganda-malawi-sign-pact-fight-cybercrime-build-capabilities/article/1475276

SADC. (2018). *SADC ICT Sub-Committee (SCOM) Meeting SADC Headquarters, Gaborone, Botswana*. Retrieved from https://www.sadc.int/files/5315/3139/7850/Media_Release.pdf

SAHRC. (2017, August). *South African Human Rights Commission Submission on the Cybercrimes and Cybersecurity Bill [B6-2017].* Retrieved from Elipses: https://www.ellipsis.co.za/wp-content/uploads/2017/09/Cybercrimes_Cybersecurity_Bill_2017_SAHRC.pdf

Saki, O. (2017). *MISA Zimbabwe Commentaries on The Cyber Crime and Cyber Security Bill, 2017.* Retrieved from Media Institute of Southern Africa Zimbabwe Chapter: https://crm.misa.org/upload/web/misa-zimbabwe-commentaries-on-the-cybercrime-and-cyber-security-bill-2017_december-2018.pdf

Saran, S. (2016). Striving for an International Consensus on Cyber Security: Lessons from the 20th Century. *Global Policy, 7*(1), 93-95.

Schjølberg , S., & Ghernaouti-Hélie, S. (2009). *A Global Protocol on Cybersecurity and Cybercrime: An initiative for peace and security in cyberspace.* Cybercrime Data.

Serianu. (2016). *Africa Cyber Report 2016.* Retrieved from Serianu: https://www.serianu.com/downloads/AfricaCyberSecurityReport2016.pdf

Shires, J. (2018). Enacting Expertise: Ritual and Risk in Cybersecurity. *Politics and Governance, 6*(2).

Smith, B. (2017, February 14). *The Need for a Digital Geneva Convention.* Retrieved from Microsoft: https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/#sm.00018k1n01i3tfomwyo20tis4co2l

Smith, B. (2018, November 12). *An important step toward peace and security in the digital world.* Retrieved from Microsoft: https://blogs.microsoft.com/on-the-issues/2018/11/12/an-important-step-toward-peace-and-security-in-the-digital-world/

Standard, B. (2018, June 25). *India, Seychelles sign pacts for cooperation in cyber security and sharing of white shipping info*. Retrieved from Business Standard: https://www.business-standard.com/article/pti-stories/india-seychelles-sign-pacts-for-cooperation-in-cyber-security-and-sharing-of-white-shipping-info-118062500903_1.html

Sund, C. (2007). Towards an international road-map for cybersecurity. *Online Information Review, 31*(5).

Sutherland, E. (2017). Governance of cybersecurity - The case of South Africa. *African Journal of Information and Communication, 20*.

Tanczer, L. M., Brass, I., & Carr, M. (2018). CSIRTs and Global Cybersecurity: How Technical Experts Support Science Diplomacy. *Global Policy*, 60-66.

Tanzania Ministry of Transport. (2003). *National Information, Communications Technologies Policy.* Retrieved from TZ Online: http://www.tzonline.org/pdf/ictpolicy2003.pdf

The Commonwealth. (2019). *Commonwealth Cybercrime Initiative*. Retrieved from The Commonwealth: https://thecommonwealth.org/commonwealth-cybercrime-initiative

Trucano, M. (2016). *SABER-ICT Framework Paper for Policy Analysis: Documenting national educational technology policies around the world and their evolution over time.* Retrieved from World Bank Education, Technology & Innovation: SABER-ICT Technical Paper Series:

https://openknowledge.worldbank.org/bitstream/handle/10986/26107/112899-WP-SABER-ICTframework-SABER-ICTno01.pdf?sequence=1&isAllowed=y

Tsandzana, D. (2016, May 16). *The Government of Mozambique is "Spying on its Citizens", According to @Verdade*. Retrieved from Advox: Global Voices: https://advox.globalvoices.org/2016/05/16/the-government-of-mozambique-is-spying-on-its-citizens-according-to-verdade/

U.S State Department. (2015, September 22). *United States and Mozambique Host Cybersecurity and Cybercrime Workshop in Maputo*. Retrieved from United States Africa Command: https://www.africom.mil/media-room/Article/26596/united-states-and-mozambique-host-cybersecurity-and-cybercrime-workshop-in-maputo

UNCTAD. (2019). *Summary of Adoption of E-Commerce Legislation Worldwide*. Retrieved from United Nations Conference on Trade and Development: https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Global-Legislation.aspx

UNIDR. (2019). *Cyber Policy Portal*. Retrieved from United Nations Institute For Disarmament Research: https://cyberpolicyportal.org/en/

Vodafone. (2018). *Sustainable Business Report 2018.* Retrieved from Vodafone: https://www.vodafone.com/content/dam/vodcom/sustainability/pdfs/sustainablebusiness2018.pdf

Vodafone. (2019). *Sustainable Business Report 2019.* Retrieved from Vodafone: https://www.vodafone.com/content/dam/vodcom/sustainability/pdfs/sustainablebusiness2019.pdf

World Bank. (2016). *OECS Countries - E-government for Regional Integration Program Project .* Retrieved from World Bank Group: http://documents.worldbank.org/curated/en/203141473933568199/OECS-Countries-E-government-for-Regional-Integration-Program-Project

Zambia National ICT Policy. (2006). *National Information Communication and Technology Policy.* Retrieved from The Zambian - Ministry of Communications and Transport: https://thezambian.com/wp-content/uploads/2007/04/Zambia-Information-and-Communication-Technology-Policy.pdf

ZTE. (2019, May 29). *ZTE releases a 5G security white paper at GSMA Mobile 360 Security for 5G.* Retrieved from ZTE: https://www.zte.com.cn/global/about/news/20190529e1.html