Norwegian Institute of International Affairs

POLICY BRIEF – 6 / 2021

Digital technology and development

Part 1 of 4 in the series: Digital technology and international politics

Erik Kursetgjerde and Niels Nagelhus Schia

RECOMMENDATIONS

- While the African Union is a relevant actor for coordinating and facilitating actions aimed at addressing cyber-related issues, assistance is needed from countries with a presence in the region that have high levels of digital competency.
- It is mutually beneficial for active donors with high digitalization competencies, such as Norway, to partner with sub-Saharan African countries in cyber capacity building. This can be done via the development aid network, and will also provide access to fast-growing digital markets.
- Norway has a specific focus on digital transformation within its development policy, the aim being to assist developing countries in taking full advantage of digital technologies[1]. Helping countries strengthen their digital capacities and national autonomy will also facilitate the development of transparent value chains, which in turn can help support human rights and freedom of speech, as well as highlight issues of modern slavery.
- To gain effective reach, awareness-raising and capacity-building efforts must be applied across multiple initiatives. Here, particular focus should be placed on children, teachers, researchers, decision-makers and private sector actors.
- The internet is only as strong as its weakest link. States and other relevant actors must ensure that cyberspace and the digital infrastructure it is reliant on are robust enough to meet an ever increasing threat profile. Here, the Cybersecurity Maturity Model for Nations (CMM)[2] offers a useful example of the steps states can take in understanding what works and what doesn't when it comes to cyber capacity building.
- Support must be provided to bolster regional capacity-building partners if cyber capacity building across sub-Saharan Africa is to be strengthened.[3]

Digitalization and cybersecurity as new global challenges

Increasingly, the global challenges posed by digitalization and cybersecurity are emerging as central to the organization of development assistance – with consequences for billions of people in the developing world. The distribution of digital technology and connectivity is occurring at an unprecedented pace, offering new opportunities and contributing to economic growth across the world. While development agencies and donor countries are utilizing such opportunities as a vehicle for achieving the Sustainable Development Goals (SDGs), new societal vulnerabilities are arising alongside them. These vulnerabilities have significant implications in terms of – among other things – freedom of speech, human rights, and modern forms of slavery. This is especially the case in those countries currently making the leap into the digital age, where there is a pressing need for knowledge, education, institution building and experience sharing. Sustainable growth through digital technology is dependent on analogue foundations, with donor countrieshaving an important role to play through development assistance and capacity-building mechanisms. With this in mind, this article looks at the rapid growth in internet usage in sub-Saharan Africa and its implications for governance, cybersecurity and development in the region.

The unprecedented pace of internet usage growth

Over the past couple of decades, the number of internet users in sub-Saharan Africa has risen significantly. In 2009, just 4.4% of the population in sub-Saharan Africa were using the internet; by 2019, this had increased to 26%.[4] Angola, for example, had only 30,000 internet users out of a population of 16.4 million at the end of 2000, a figure that had grown to almost 9 million users out of a population of nearly 33 million in 2019. The Seychelles, meanwhile, went from 14.5% of individuals using the internet in 2003 to 79% in 2019.

Such examples point towards the unprecedented pace of internet usage growth in the region. While this growth is impressive, major disparities exist both between countries and within them (particularly between urban and rural areas). In South Africa, over half the population have internet access, while numbers suggest only around 10% of the population in the Central African region has access – in the Central African Republic, for example, just 4% of the population were using the internet in 2016. Internet access outside major urban centres is limited, with lack of access to electricity a major barrier to those living in the most impoverished countries and rural areas. Other obstacles to meaningful access include the cost of devices, low digital literacy and data prices.

The average internet user in sub-Saharan Africa uses their mobile phone for connectivity and as their bank account, with most of the region's countries having gone from almost non-existent connectivity to widespread 3G/4G/5G mobile internet coverage. Such usage is mostly driven by a lack of infrastructure, which makes it difficult to develop and maintain broadband connections, an issue that restricts the traditional financial infrastructure used by banks. Despite the relatively low overall numbers for internet usage in sub-Saharan Africa, numbers for 2019 showed that 49% of the region's population was within the footprint of a mobile broadband network.[5]

In sub-Saharan Africa, as with the rest of the world, the COVID-19 pandemic has impacted information and communications technology (ICT) services. Preliminary research shows an increased dependence on digital infrastructure and increased digitalization of services – though these trends were already in evidence prior to the emergence of COVID, the pandemic has accelerated them still further. However, while internet connectivity can be seen to speed up economic growth and provide business, trade and commerce opportunities, a number of key issues remain to be addressed. In particular, international reports have highlighted several sub-Saharan Africa countries as being among the most affected by global cybercrime.[6] Generally, the region is viewed as a safe haven by cybercriminals and other malicious actors due to a lack of relevant regulations and laws, low cybersecurity awareness among the population, a lack of resources for cybersecurity measures, and the limited number of cybersecurity professionals.[7] The situation is further complicated by the rapid increase in the number of internet users, which has created challenges both in terms of adequate infrastructure development and in installing appropriate regulatory structures.

Efforts have been made to address these issues, including an increase in budgets related to cybersecurity, a shift in perspective towards deterring malicious actors, and a greater focus on awareness-raising, with organizations impressing on users the need to be vigilant. Moreover, the African Union (AU) has launched various initiatives aimed at addressing cybersecurity. Even so, the fact that cyberspace is a borderless domain means that comprehensive domestic strategies, combined with regional and international cooperation, are required to manage the negative impacts of increased digitalization.

If appropriate regulations and security frameworks are not put in place to secure the cybersecurity of digital infrastructure in sub-Saharan Africa, there is a risk that the region's ICT boom could actually impede economic growth, thereby undermining progress among some of the world's poorest countries towards the SDGs. Turning new regulations, frameworks and laws into practice, however, requires substantial awareness-raising efforts and digitally competent bureaucracies. Given this, it is vital that countries in the region take the opportunity to invest in education and research that will strengthen their cyber capabilities.

Internet governance, the African Union, and how best to cope with rapid digitization

International frictions on how the internet should be governed represent a complicating factor in addressing the issues raised above. Ideological divisions between great powers on standardization of data protection and internet usage make it difficult for sub-Saharan states to press their cyber-policy positions on the wider international stage, where power politics often comes into play. For this reason, a more regional approach appears to be the more fruitful avenue, with the AU playing the role of facilitator and key actor.

The AU has already played an agenda-setting role when it comes to international cooperation within the cyber domain, encouraging information-sharing and the sharing of best practices between states, and putting the focus

on wider cybersecurity challenges. Unfortunately, a lack of compliance from AU member states has hampered progress in this arena, with negative knock-on effects for sub-Saharan economies – ultimately, it is member states who decide how to interpret conventions and implement laws at a national level.

The 2001 Budapest Convention on Cybercrime has been discussed as a possible measure that could be implemented in African countries. However, only a handful of sub-Saharan countries (Cabo Verde, Mauritius, Ghana and Senegal) have ratified the convention, which is perhaps unsurprising given that countries from the region were not involved in negotiations. Other voices have raised the prospect of an Addis Ababa Convention organized and coordinated by the AU. However, given there is already an AU Convention on Cyber Security and Personal Data Protection, which only a few countries have ratified, the likelihood of such a process succeeding is uncertain at best. A number of reasons have been offered regarding the lack of support thus far for the AU Convention, the most obvious of which is a lack of understanding of digitalization and its consequences, which feeds into a lack of political will.[8]

Such trends have the effect of limiting the digital sovereignty enjoyed by these countries, which in turn opens up economies in the region to further exploitation by multinational companies and powerful states, and, through a lack of transparency, enables modern slavery. An example is Facebook's Free Basics initiative, which provides limited internet access free of data charges. As well as challenging the net neutrality principle , a number of data protection issues arise, especially as most countries in sub-Saharan Africa have little or no regulation in place. By contrast, countries in Europe have had data protection high up the agenda for over a decade, as evidenced by the European Union (EU)'s General Data Protection Regulation (GDPR). Moreover, the EU's proposed Digital Markets Act (DMA) and Digital Services Act (DSA) aim to target the lack of competition in digital markets and ensure transparency and consumer protection.

The severity and complexity of the digital challenges faced by countries in sub-Saharan Africa is highlighted by the fact that developed, highly digitized countries in Europe are struggling with many of the very same issues. Given this, drawing on European and international experiences may provide grounds for optimism in an African context, as they can be used to inform the building of new institutions and regulations, thereby providing a head-start in the race for digital development.

Within the sub-Saharan region, Kenya, Rwanda, South Africa and Mauritius have been rated with high legal, technical and organizational competencies in the cyber domain. Other African countries should therefore work with these states to establish a convention aimed at mitigating cybercrimes. It is the countries with the weakest cybercrime laws that have suffered the greatest losses to their economies , relative to their gross domestic product (GDP). An example is Nigeria, which has experienced 500 million USD in losses suffered annually by cybercrime. Therefore, they should be included and assisted in relevant discussions at a much larger scale.

Another reason countries are paying insufficient attention to cybersecurity policy is that they lack the means to evaluate the damage done to their economies. While a cybercrime incident may be reported in the media, there is rarely if ever any follow up quantifying how much was lost in terms of down-time, missed opportunities, ransom payments or cost of restoration.

One means of moving cybersecurity up the agenda in the region is through international cooperation. Countries across the globe have – or should have – a significant interest in assisting other countries with their cybersecurity, as the internet is only as strong as its weakest link. A country with weak digital infrastructure and security may be used as a proxy by other states or actors to launch cyberoperations. Thus, if one does not ensure that cybersecurity capacity exists across all states, there is a risk of a vacuum being created within which foreign actors can easily and with impunity conduct malicious cyberoperations. Furthermore, the country used as a proxy will likely be blamed either for the cyberoperation itself or for having failed to secure its digital infrastructure.

Conclusions

Many sub-Saharan Africa states are struggling to keep up with the development nexus of growing economies and increased connectivity, and as such face significant challenges in handling the digital domain. The Cybersecurity Capacity Maturity Model for Nations (CMM) is one model aimed at helping states understand what works, what doesn't, and why, when it comes to cybersecurity capacity building.[9] Applying the framework provides governments and enterprises with a tool that can assist in adopting relevant policies and making investments that enhance cyber safety and security, while also respecting citizens' human rights, such as privacy and freedom of expression. Doing so will ultimately benefit the states involved by improving the resilience of their cyber governance and cybersecurity systems.

Cyber capacity building aims to build functioning and accountable institutions that can respond to cybercrime and improve a country's cyber resilience. Countries with weak cybercrime laws are suffering significant losses to their economies as a result, and so efforts should be made to include and assist them in relevant discussions. In this regard, CMM offers an excellent platform to develop knowledge and understanding, with the failure thus far of the Budapest Convention on Cybercrime and the AU Convention on Cyber Security and Personal Data Protection explainable by a lack of comprehension as to preferred policy or the urgency of action.

In supporting implementation of the CMM recommendations, there is great potential for donor countries to build up digital competencies in countries receiving development assistance – while also gaining access to an emerging market. Such an approach would be very much in line with current development policy priorities in donor countries. McKinsey projects Africa's e-commerce market will reach US$75 billion by 2025 , and that the internet will foster a US$300 billion increase in the continent's GDP through increased productivity in sectors such as finance, agricul-

ture, education, health, retail and government[10]. The internet of things (IoT) holds great potential for the region given that it allows for the leapfrogging of infrastructure-reliant communications – as such, countries should in theory be able to adopt IoT solutions at a faster pace.

Many countries in sub-Saharan Africa have already started down the path of building up digital competencies, with universities launching initiatives aimed at training young Tas and PhDs in cybersecurity. Similar courses on the connections between digital technology, policy spaces and impacts on society (including on human rights and freedom of speech) are, however, lagging. In terms of capacity development, cybersecurity is seen as a technical area – as a consequence, both academia and organizations have failed to prioritize policy and strategy. In the private and public sectors, cybersecurity is generally subordinated under IT, or under the risk office. Within the government policy space, it is often the case that there is no dedicated person dealing with cybersecurity policy issues, only technically oriented personnel who are for the most part unfamiliar with policy development.

As such, there is a great need for dedicated national cyber programmes. These can be developed alongside donor partners, such as Norway, and supported through development budget allocation. Countries with digital resources and e-governance experience should also push for greater acceptance of cybersecurity as a development issue within the broader development community. This would help foster common understanding and enable the putting in place of a framework robust enough to deal with the emerging cyber challenges faced by different stakeholders.

The International Telecommunication Union (ITU) Global Cyber Security Index (GCI) supports the claim that most sub-Saharan countries – Kenya, Mauritius, Rwanda and South Africa excepted – have low levels of cyber maturity. This holds true across the full spectrum of the index, from governance levels to responsiveness and development. Cybersecurity below the poverty line therefore equates to a scarcity of resources relative to the scale of threat. At present, few African states have a national cybersecurity strategy or the necessary policies and laws in place to deal with cybersecurity and data protection. In terms of addressing this, the UK's Foreign Secretary, Dominic Raab, recently announced a £22 million investment aimed at strengthening cybersecurity resilience in developing countries in Africa and the Indo-Pacific. Norway, meanwhile, has signalled its intention to strengthen support for cybersecurity capacity building (including institution building, rule of law and digital infrastructure) in developing countries.[11]

The rising number of cyberoperations targeting countries in sub-Saharan Africa highlights the importance of a comprehensive approach to meeting cyber threats to the region. Unfortunately, both the private and public sectors are only just beginning to identify and respond to this development. African governments need to take urgent steps towards increasing their cybersecurity capabilities through formulating national strategies and policies, and creating CIRTs (Computer Incident Response Teams) that meet international standards. In embarking on this process, it will be necessary to go beyond merely using expertise and practices taken from abroad – standards relevant to the region's cultural and societal contexts must be developed if long-tern success is to be achieved.

1'Digital transformasjon og utviklingspolitikken', Report to the Storting (white paper), Meld. St. 11 (2019–2020), 2019, www.regjeringen.no/no/dokumenter/meld.-st.-11-20192020/id2682394/?ch=3#kap6.
2 'Cybersecurity Capacity Maturity Model for Nations (CMM): 2021 edition', Global Cyber Security Capacity Centre, 2021, https://gcscc.ox.ac.uk/the-cmm#/.
3 See, for example, the Cybersecurity Capacity Centre for Southern Africa (C3SA): https://c3sa.uct.ac.za.
4 The World Bank, 'Individuals using the Internet (% of population) - Sub-Saharan Africa', https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=ZG.
5 GSMA, 'Mobile Internet Connectivity 2020: Sub-Saharan Africa Factsheet', 2020, www.gsma.com/r/wp-content/uploads/2020/09/Mobile-Internet-Connectivity-SSA-Fact-Sheet.pdf.
6 See for instance the World Bank Report Digital Dividends (2015).
7 Trend Micro, 'Africa: A New Safe Habor for Cybercriminals?', 15 April 2013, https:// blog.trendmicro.com/africa-a-new-safe-harbor-for-cybercriminals/.
8 Tomslin Samme-Nlar, 'Why it is Important for African States to Ratify the Malabo Convention', African Academic Network on Internet Policy, 31 July 2021, https://aanoip.org/why-it-is-important-for-african-states-to-ratify-the-malabo-convention/; Nigerian Post, 2020 Ratifying Pan-African Parliament Malabo Protocol - The Nigerian Post.
9 'Cybersecurity Capacity Maturity Model for Nations (CMM): 2021 edition', Global Cyber Security Capacity Centre, 2021, https://gcscc.ox.ac.uk/the-cmm#/.
10 Lions go digital: The Internet's transformative potential in Africa, McKinsey, 2013, https://www.mckinsey.com/~/media/mckinsey/industries/technology media and telecommunications/high tech/our insights/lions go digital the internets transformative potential in africa/mgi_lions_go_digital_full_report_nov2013.pdf
11 'Digital transformasjon og utviklingspolitikken', Report to the Storting (white paper), Meld. St. 11 (2019–2020), 2019, www.regjeringen.no/no/dokumenter/meld.-st.-11-20192020/id2682394/?ch=3#kap6.

Erik Kursetgjerde is an advisor for the Ministry of Local Government and Modernisation.
Niels Nagelhus Schia is a senior research fellow and manager for NUPI's Center for Cyber Security Studies.

Norwegian Institute of International Affairs

NUPI
Norwegian Institute of International Affairs
C.J. Hambros plass 2D
PB 7024 St. Olavs Plass, 0130 Oslo, Norway
www.nupi.no | post@nupi.no

Established in 1959, the Norwegian Institute of International Affairs [NUPI] is a leading independent research institute on international politics and areas of relevance to Norwegian foreign policy. Formally under the Ministry of Education and Research, NUPI nevertheless operates as an independent, non-political instance in all its professional activities. Research undertaken at NUPI ranges from shortterm applied research to more long-term basic research.

Photo: Anton Balazh, Adobe Stock 2021