INSTITUTE FOR SECURITY STUDIES

POLICY BRIEF 73 | JANUARY 2015

The AU's cybercrime response

A positive start, but substantial challenges ahead

Eric Tamarkin

Recommendations

1 African states should ratify the AU Convention on Cyber Security and Personal Data Protection.

2 African states should prioritise the implementation of the cybercrime aspects of the convention by enacting comprehensive and harmonised cybercrime laws and enhancing formal and informal international cooperation.

3 The AU should support capacity-building so that African states can adopt cybercrime provisions and bolster cybersecurity.

4 The AU should provide robust oversight of the implementation of the convention.

5 African states should not wait for the convention process to address deficiencies in cybersecurity and gaps in their capacity to fight cybercrime.

6 African states pursuing ratification of the AU convention should also take steps to ratify the Council of Europe's Budapest convention, as cybercrime is a global problem that cannot be addressed on the continent alone.

Summary

African governments, the private sector and individuals increasingly rely on the Internet to conduct sensitive transactions and store important data. Most African states are lagging behind in strengthening cybersecurity and fighting cybercrime; cybercriminals have recognised this vulnerability and are targeting the continent. After a lengthy process, the African Union (AU) recently responded to the surge in cybercrime by adopting the Convention on Cyber Security and Personal Data Protection. Stakeholders have raised several concerns about the convention, including that it is too broad in scope. African states should focus on the convention's cybersecurity and cybercrime provisions first, as it is unrealistic to expect states to implement the entire convention in a timely manner. Additionally, African states must embrace capacity-building efforts and join international cybercrime agreements that reach beyond the African continent. These steps will have the most immediate effect in curbing the growth of cybercrime in Africa and worldwide.

INTERNET PENETRATION IS growing exponentially in Africa and around the globe. According to the International Telecommunication Union, by the end of 2014, 'there will be almost 3 billion Internet users, two-thirds of them coming from the developing world'.[1] In Africa, almost 20% of the population will have Internet access by the end of 2014, up from 10% in 2010.[2]

Much of this growth has been fuelled by a dramatic increase in the use of mobile technology, particularly in Africa. A recent study by technology company Ericsson found that Internet use on mobile phones in sub-Saharan Africa was expected to increase 20-fold between the end of 2013 and the end of 2019. This is double the rate of growth in the rest of the world.[3] Ericsson determined that by the end of 2014, there

would be over 635 million mobile subscriptions in sub-Saharan Africa, and by the end of 2019 the number of subscriptions in the region was expected to reach about 930 million.[4]

While increased Internet connectivity is revolutionising daily interactions between individuals, businesses and governments, it has also provided an opening that criminals can exploit. According to a June 2014 study by information and communications technology (ICT) security company McAfee and the Center for Strategic and International Studies, the 'annual cost to the global economy from cybercrime is more than [US]$445 billion'.[5] Because the Internet is 'globally connected, borderless, anonymous, fast, low-risk, easily accessible and has high volumes of rich data including financial data, personal information, military information and business information', organised criminal entities are increasingly attracted to cybercrime.[6] Organised cybercrime groups now have technical capacity rivalling that of nation states. They can build 'complex systems aimed at stealing money and intellectual property on a grand scale, costing almost the same to the global economy as counterfeiting or the narcotics trade'.[7]

> African states that fail to adequately address the evolving cybercrime problem will jeopardise their economic growth and national security

A report by TrendMicro, an ICT security company, concluded that Africa was becoming a cybercrime safe harbour because of increased Internet availability at lower costs, a rapidly growing Internet user base and a dearth of cybercrime laws on the continent.[8] Cybercriminals in Africa are not only using techniques such as the 419 scam or advance fee fraud that originated in Nigeria, but are also deploying more advanced and 'lucrative forms of cybercrime that involve the use of botnets, remote access Trojans, and banking/finance-related malware'.[9] African states that fail to adequately address the evolving cybercrime problem will jeopardise their economic growth and national security.

An effective multilayered approach to combating cybercrime requires the proactive participation of and cooperation between individuals, the private sector and governments. Essential elements of this approach are governments' enacting robust laws to criminalise cybercrime, harmonising their cybercrime laws, developing the capacity to enforce cybercrime laws and enhancing timely international cooperation on cybercrime investigations.

Unlike physical crimes, the perpetrators and victims of cybercrime are often in different parts of the world. According to Troels Oerting, head of Europol's Cybercrime Centre, the 'biggest issue facing cybercrime fighters is the fact that cybercrime is borderless'. He noted that because 'criminals … commit their crimes from a distance', Europol 'cannot use the normal tools to catch them'.[10] The transnational nature of most cybercrime adds complexities of 'sovereignty, jurisdiction, extraterritorial evidence and international cooperation'.[11] The additional challenges faced in ensuring international cooperation on fighting cybercrime include 'extradition, mutual legal assistance, mutual recognition of foreign judgments, and informal police-to-police cooperation'.[12]

Through the recent adoption of the AU Convention on Cyber Security and Personal Data Protection, the AU took a positive step in addressing some of these problems.

27 JUNE 2014

THE AFRICAN UNION ADOPTS THE AU CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION

However, the AU faces significant hurdles in convincing all African states to ratify the convention and implement its provisions. Furthermore, some of the convention's cybercrime provisions remain controversial and it fails to tackle the fact that fighting cybercrime requires international cooperation reaching beyond Africa's geographical borders.

The AU convention's circuitous procedural history

The AU adopted the convention on 27 June 2014, at the 23rd Ordinary Session of the Summit of the AU in Malabo, Equatorial Guinea. This was the culmination of a process that started with the Oliver Tambo Declaration at the Extraordinary Session of the AU Ministers in charge of ICT in November 2009 in Johannesburg. This declaration asked that the AU Commission 'jointly develop with the United Nations Economic Commission for Africa … a convention on cyber legislation based on the Continent's needs and which adheres to the legal and regulatory requirements on electronic transactions, cyber security, and personal data protection'.[13] It also recommended 'that AU Member States adopt this convention by 2012'.[14]

After consultations and regional workshops that engaged African stakeholders and international experts, the AU Commission released a draft convention that was endorsed by the AU Conference of Ministers in charge of ICT in Khartoum in September 2012.[15] The convention was slated for consideration at the AU Summit in January 2014, but the AU abruptly removed it from the agenda over concerns raised by the private sector, civil society organisations and privacy advocates,[16] including the Kenya ICT Action Network, the Kenyan and Ugandan chapters of the Internet Society, the I-Network in Uganda and the Collaboration on International ICT Policy in East and Southern Africa.[17] Curiously, the convention was tucked away in a 194-page legal instrument that was finally adopted in June 2014 with little fanfare or discussion.

Cybercrime provisions in the AU convention

The convention attempts to address a wide range of online activities, including electronic commerce, data protection, cybersecurity and cybercrime. Regarding cybercrime, it requires African states to adopt laws that criminalise:

- Attacks on computer systems (e.g. fraudulently accessing a computer system)
- Computerised data breaches (e.g. fraudulently intercepting data)
- Content-related offences (e.g. disseminating child pornography)
- Offences relating to electronic message security measures

Furthermore, the convention emphasises the importance of enhancing international cooperation to fight cybercrime. Article 28 requires states to harmonise cybercrime legislation and regulations to 'respect the principle of double criminal liability'.[18] In order to facilitate information-sharing across borders and enhance collaboration on a bilateral and multilateral basis, the convention calls on states without cybercrime mutual legal assistance agreements to try to rectify this deficit.[19]

The convention recognises that building capacity to fight cybercrime is essential, requiring African states to 'establish appropriate institutions to combat cybercrime' and to offer training to those stakeholders tasked with fighting cybercrime.[20]

Additionally, it requires that African states enact cybercrime offences that 'are punishable by effective, proportionate and dissuasive criminal penalties'.[21] The convention thus rightly emphasises the need to create sufficient deterrents to reverse the status quo of criminals turning to cybercrime because it is low risk.

Article 32 designates the AU Commission Chairperson as responsible for overseeing the establishment and monitoring of the convention. Among other responsibilities, the Chairperson is required to:

- Encourage African states to adopt and implement the convention's measures
- Advise African states on how to promote cybersecurity and combat the scourge of cybercrime at a national level
- Analyse the nature and magnitude of cybercrime, including gathering information about cybercrime activity in Africa and transmitting such information to the competent national authorities
- Establish partnerships with African civil society and governmental, intergovernmental and non-governmental organisations in order to facilitate dialogue on combating cybercrime
- Submit regular reports on the progress made by each African state in the implementation of the convention's provisions[22]

Fifteen countries must ratify the convention before it enters into force. To date, no countries have done so and the AU faces substantial challenges in convincing states to support the convention and implement its provisions.

Concerns over and challenges with the AU approach

The convention deserves praise for prioritising the need for African states to address the problem of cybercrime and tackle deficiencies in their cybersecurity. However, it is unclear whether the concerns that had delayed the convention's consideration in January 2014 have been adequately addressed.

For example, one Kenyan advocacy group criticised the content-related offences section as imposing 'dangerously broad limitations on free speech'.[23] The draft language that led to those concerns appears to remain substantially unchanged in the final version. In particular, free speech critics of the AU's approach cite the provision that requires the criminalisation of the computerised creation and dissemination of 'writings, messages, photographs, drawings or any other presentation of ideas or theories of racist or xenophobic nature'.[24] Additionally, free speech critics object to the required criminalisation of using a computer system to 'insult … persons for the reason that they belong to a group distinguished by race, colour, descent, national or ethnic origin, or religion or political opinion'.[25] Finally, they question the required criminalisation of using a computer system to 'deliberately deny, approve or justify acts constituting genocide or crimes against humanity'.[26]

There are further concerns that the scope of the convention is overly ambitious and too cumbersome, as it deals with many areas of electronic activity beyond cybercrime. The few African states that have enacted cybercrime laws, including Cameroon, Kenya, Mauritius, South Africa and Zambia, will have to engage in an arduous process to reconcile differences between their laws and the convention's requirements.[27] The vast majority of African states without cybercrime laws will have to draft cybercrime legislation from scratch. This process will be difficult given the lack of awareness about cybercrime in Africa, the inherent complexities of the problem and deficiencies in capacity across the continent.

> The vast majority of African states without cybercrime laws will have to draft cybercrime legislation from scratch

THERE ARE DEFICIENCIES IN THE TRAINING OF POLICE, PROSECUTORS AND JUDGES AS WELL AS IN DEVELOPING INVESTIGATIVE METHODS FOR COMPUTER-RELATED CRIMES AND ELECTRONIC CRIMINAL EVIDENCE

Capacity shortfalls are a particularly challenging hurdle to the timely implementation of the convention's cybercrime provisions. Many African states lack the technical expertise to draft and enforce such laws. Furthermore, there are deficiencies in the training of police, prosecutors and judges as well as in developing investigative methods for computer-related crimes and electronic criminal evidence. According to a cybercrime study by the United Nations Office on Drugs and Crime (UNODC), every country in Africa that responded to its questionnaire indicated a need for technical assistance.[28] Respondents sought assistance in international cooperation and prosecution, computer forensics and evidence, general cybercrime investigations and trial support.[29]

The AU has recognised these challenges and tasked the New Partnership for Africa's Development (NEPAD) with developing and implementing a capacity-building project that closes the following capacity gaps:

- Shortage of expertise and resources to help African states ratify and transpose the convention and monitor progress

- Lack of cybercrime and cybersecurity legal and regulatory environments in African states
- Shortage of a high-quality cybersecurity workforce and of public and private leadership
- Deficiencies in educational and training platforms required to develop and support a future cybersecurity workforce
- Limited availability and use of technology, processes, business models and standards to manage cyber risks to individuals, the private sector and governments[30]

Unfortunately, NEPAD may not have the necessary resources to fund this plan and, as a result, the burden of capacity building may fall on traditional development partners outside Africa. For example, the United States recently hosted a sub-Saharan African cybersecurity and cybercrime workshop in Botswana at which 15 Southern African states were represented.[31] Among other issues, the programme focused on mobile device security, a key concern for the continent given the tremendous growth in mobile technologies in Africa.

Too many international cybercrime instruments?

The AU convention faces another challenge in that it joins a crowded field of bilateral and multilateral cybercrime conventions, draft frameworks and model laws. In Africa, regional economic communities (RECs) have developed the following:

- East African Community (EAC) Draft Legal Framework for Cyberlaws (2008)
- Economic Community of West African States (ECOWAS) Draft Directive on Fighting Cybercrime (2009)
- Common Market for Eastern and Southern Africa (COMESA) Cyber Security Draft Model Bill (2011)
- Southern African Development Community (SADC) Model Law on Computer Crime and Cybercrime (2012)

The EAC draft legal framework, the COMESA draft model bill and the SADC model law are non-binding instruments that are 'not intended to create legal obligations for states'.[32] Instead, these instruments 'are designed to serve as inspiration or models for [the] development of national legislative provisions'.[33] In contrast, the AU convention and the ECOWAS directive are binding measures that create legal obligations on member states. Regardless of their form, instruments developed by RECs have had difficulty gaining support in their respective regions. Whether the AU convention will have more success across the continent is yet to be determined.

In addition to the competing cybercrime instruments in Africa, there is an array of other international instruments initiated outside the continent. The Council of Europe's Convention on Cybercrime (the Budapest convention), which opened for signature on 23 November 2001 and entered into force on 1 July 2004, is the most broadly supported. To date, 44 states have ratified the Budapest convention, but Mauritius is the only African state to have taken that step. South Africa signed the Budapest convention in November 2001 but has yet to ratify, and Morocco[34] and Senegal are in the process of joining. Besides specifying cyber acts that should be criminalised, the Budapest convention requires that states harmonise their cybercrime laws, develop the capacity to investigate online crimes and establish mechanisms to facilitate formal and informal international cooperation.

> It is not surprising that the AU convention's language has generated similar free speech concerns

The Council of Europe has also adopted the Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. This additional protocol, which was opened for signature on 28 January 2003 and entered into force on 1 March 2006, was separated from the core provisions of the Budapest convention in response to free speech concerns raised by several states. Thus far only 22 countries have ratified the additional protocol. While no African states have ratified it, South Africa became a signatory as of April 2008. Since the cybercrime provisions of the AU convention contain similar language as the additional protocol, it is not surprising that the AU convention's language has generated similar free speech concerns.

In a competing instrument adopted in 2009, China, Russia, Kazakhstan, Kyrgyzstan, Tajikistan and Uzbekistan endorsed the Shanghai Cooperation Organization Agreement on Cooperation in the Field of International Information Security. Rather than specifying cyber acts that should be criminalised or identifying ways to enhance international cooperation, this agreement is a broad policy document that focuses on 'information security'.[35] Parties to this agreement seek to reframe the cybercrime debate by emphasising the need to enact controls to block online content that could destabilise a state's political, economic and social systems.

Russia and China also backed an unsuccessful effort in 2010 to create a new United Nations treaty on cybercrime that

focused on information security. They are currently negotiating a bilateral agreement on cybersecurity that is expected to be finalised in early 2015.

A problem with regional or bilateral cybercrime instruments is that they create a cooperation cluster that is unable to address the global nature of cybercrime.[36] Under the current system, states that are not parties to the same agreement are restricted to traditional modes of international cooperation that fail to provide the mechanisms to handle the real-time information-sharing and data-preservation aspects of electronic evidence.[37]

Conclusion

Despite the substantial hurdles and shortcomings of the international treaty approach, states that coalesce around a common instrument will have a stronger position in the global fight against cybercrime. So long as there remains a weak link in the cybersecurity chain, cybercriminals will seek to exploit it. Unless and until there is broad global agreement on criminalising cybercrime and robust international cooperation to enforce those laws, cybercriminals operating in cybercrime safe havens will continue to target individuals, businesses and governments with impunity.

If Africa becomes known as a cybercrime safe harbour, this could have devastating consequences for the continent's potential growth. Furthermore, if an African state becomes known as a hospitable environment for cybercriminals, it will not only damage that country but will also have a negatively impact on the reputation of the continent as a whole. The AU's convention is a positive step toward prodding African states into taking proactive domestic measures to help curb the scourge of cybercrime. The Budapest convention remains the best available instrument to unite the international community under a common framework to fight cybercrime, but African states should not wait for the international cybercrime treaty process to unfold, as ratification is not a panacea to the cybercrime problem. They should instead focus on shoring up their cybersecurity and enhancing their capacity to fight cybercrime without delay.

Notes

1 International Telecommunication Union, ITU releases 2014 ICT figures, 5 May 2014, www.itu.int/net pressoffice/press_releases/2014/23.aspx#.VHhUsSiB3S8.

2 Ibid.

3 Ericsson, *Sub-Saharan Africa: Ericsson Mobility Report Appendix,* June 2014, www.ericsson.com/res/docs/2014/emr-june2014-regional-appendices-ssa.pdf.

4 Ibid.

5 Center for Strategic and International Studies and McAfee, *Net losses: estimating the global cost of cybercrime: economic impact of cybercrime II,* June 2014, www.mcafee.com/ca/resources/reports/rp-economic-impact-cybercrime2.pdf.

6 Australian Crime Commission, Organised crime: cybercrime, www.crimecommission.gov.au/organised-crime/crime-enablers-and-pathways/cybercrime.

7 S. Ranger, Organised cybercrime groups are now as powerful as nations, *ZDNet,* 9 June 2014, http://www.zdnet.com/organised-cybercrime-groups-are-now-as-powerful-as-nations-7000030323/.

8 L. Kharouni, Africa: a new safe harbor for cybercriminals?, Trend Micro Inc., Research Paper, 2013, www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-africa.pdf.

9 Trend Micro, Checking in on Africa: the latest developments in cybercrime, 11 August 2014, http://blog.trendmicro.com/trendlabs-security-intelligence/checking-in-on-africa-the-latest-developments-in-cybercrime/.

AFRICAN STATES SHOULD NOT WAIT FOR THE INTERNATIONAL CYBERCRIME TREATY PROCESS TO UNFOLD, AS RATIFICATION IS NOT A PANACEA TO THE CYBERCRIME PROBLEM

10 Only 100 cybercrime brains worldwide says Europol boss, BBC News, 10 October 2014, www.bbc.com/news/technology-29567782.

11 United Nations Office on Drugs and Crime (UNODC), *Comprehensive study on cybercrime: draft – February 2013,* February 2013, xxiv, www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

12 Ibid., xxv.

13 African Union (AU), Oliver Tambo Declaration, Johannesburg, South Africa, 5 November 2009, http://africainonespace.org/downloads/TheOliverTamboDeclaration.pdf.

14 Ibid.

15 AU, Report on experts' session, Khartoum, Sudan, 2–4 September 2012, http://pages.au.int/sites/default/files/Report%20of%20Experts_Khartoum_CITMC4_EN_Final_0.pdf.

16 E Kenyanito, Africa moves towards a common cyber security legal framework, Access Blog, 2 June 2014, www.accessnow.org/blog/2014/06/02/africa-moves-towards-a-common-cyber-security-legal-framework.

17 Ibid.

18 AU, Convention on Cyber Security and Personal Data Protection, 30, https://www.ccdcoe.org/sites/default/files/documents/AU-270614-CSConvention.pdf.

19 Ibid.

20 Ibid., 29–30.

21 Ibid., 33.

22 Ibid., 37.

23 Centre for Intellectual Property and Information Technology Law, Letter to the African Union, http://www.scribd.com/fullscreen/186878287?access_key=key-2gk1zf4n9bc15cqfhrbv&allow_share=true&escape=false&view_mode=scroll.

24 AU, Convention on Cyber Security and Personal Data Protection, 33,https://www.ccdcoe.org/sites/default/files/documents/AU-270614-CSConvention.pdf.

25 Ibid., 32.

26 Ibid.

27 According to the Global Centre for Information and Communication Technologies in Parliament, only five African countries have enacted cybercrime laws: Cameroon's Cybersécurité et la Cybercriminalité au Cameroun (2010), Kenya's Communications (Amendment) Act (2009), Mauritius' Computer Misuse and Cybercrime Act (2003), South Africa's Electronic Communications and Transactions Act (2002), and Zambia's Computer Misuse and Crimes Act (2004).

28 UNODC, *Comprehensive study on cybercrime: draft – February 2013,* February 2013, 178, www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf. Eleven African countries responded to the UNODC cybercrime questionnaire.

29 Ibid.

30 The New Partnership for Africa's Development e-Africa Programme Infrastructure Strategic Business Unit, Draft cyber security capacity building project, October 2014.

31 United States State Department, Sub-Saharan African Cybersecurity and Cybercrime Workshop, 4–6 June 2014, http://www.state.gov/r/pa/prs/ps/2014/06/227125.htm.

32 UNODC, *Comprehensive study on cybercrime: draft – February 2013,* February 2013, 65, www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

33 Ibid.

34 Morocco is not a part of the AU and thus not eligible to ratify the AU convention.

35 UNODC, *Comprehensive study on cybercrime: draft – February 2013,* February 2013, 69, www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

36 Ibid., 215.

37 Ibid.

About the author

Eric Tamarkin is an independent researcher. He previously served as a Senior Counsel to the United States Senate Homeland Security and Governmental Affairs Committee, where he specialised in cybersecurity policy.

About the ISS

The Institute for Security Studies is an African organisation that aims to enhance human security on the continent. It does independent and authoritative research, provides expert policy analysis and advice, and delivers practical training and technical assistance.

Acknowledgements

The ISS is grateful for support from the following members of the ISS Partnership Forum: the governments of Australia, Canada, Denmark, Finland, Japan, Netherlands, Norway, Sweden and the USA.

ISS Pretoria
Block C, Brooklyn Court
361 Veale Street
New Muckleneuk
Pretoria, South Africa
Tel: +27 12 346 9500
Fax: +27 12 460 0998
pretoria@issafrica.org

ISS Addis Ababa
5th Floor, Get House
Building, Africa Avenue
Addis Ababa, Ethiopia
Tel: +251 11 515 6320
Fax: +251 11 515 6449
addisababa@issafrica.org

ISS Dakar
4th Floor, Immeuble Atryum
Route de Ouakam
Dakar, Senegal
Tel: +221 33 860 3304/42
Fax: +221 33 860 3343
dakar@issafrica.org

ISS Nairobi
Braeside Gardens
off Muthangari Road
Lavington, Nairobi, Kenya
Cell: +254 72 860 7642
Cell: +254 73 565 0300
nairobi@issafrica.org

www.issafrica.org

ISS Policy Brief No 73

ISSN 1026-0404

9 771026 040004