NTIS/002/2014

United Nations
Economic Commission for Africa

Policy Brief

Tackling the challenges of cybersecurity in Africa

1. Introduction

The 2013 Economic Report on Africa, a joint publication of the Economic Commission for Africa (ECA) and the African Union Commission (AUC), states that "following two decades of near stagnation, Africa's growth performance has improved hugely since the start of the 21st century".[1] Since 2000, the African continent has experienced a prolonged commodity boom and a sustained growth trend. The report further states that "Africa's medium-term growth prospects remain strong, too, at for example 4.8 per cent in 2013 and 5.1 per cent in 2014".[2] Also of note, highly regarded publications, such as The Economist[3] and the International Business Times4 and organzations, such as the African Development Bank (AfDB)5, have asserted that Africa is home to some of the world's most rapidly growing economies.

This new Africa, captured by the aphorism "Africa rising", is reflected in the continent's expanding middle class and rapid adoption of mobile technology. According to recent estimates by the International Telecommunications Union (ITU), the number of mobile subscribers reached 63 per cent in 2013, and more than 16 percent of the African population are now using the Internet.[6] Furthermore, it is estimated that the global value of web-based retail sales for 2013, amounted to $963 billion,[7] while business to consumer (B2C) e-commerce sales for the same period totalled $ 1.3 trillion.[8] Although the e-commerce market is dominated by developed economies, the global share of e-commerce for the Middle East and Africa is expected to rise from 1.6 per cent in 2011 to 2.3 per cent by 2016.

However, new challenges arise alongside growth, and increasing technological exposure

1 African Union Commission and United Nations, Economic Commission for Africa, *Making the Most of Africa's Commodities: Industrializing for Growth, Jobs and Economic Transformation: Economic Report on Africa 2013,* (United Nations publication), Sales No. : E.13.IIK.1., p.6.

2 Ibid.

3 J. O'S, "Growth and other good things", The Economist, 1 May 2013. Available from www.economist.com/ blogs/baobab/2013/05/ development-africa.

4 Mike Obel, "Africa poised for unprecedented, long-term economic growth: Seven drivers that could transform Africa into the world's economic powerhouse", International Business Times, 13 September 2013. Available from www.ibtimes.com/africa-poised-unprecedented-long-term-economic-growth-seven-drivers-could-transform-africa-worlds.

5 African Development Bank Group, "Africa is now the fastest growing continent in the world", 7 November 2013. Available from www.afdb.org/en/news-and-events/article/africa-is-now-the-fastest-growing-continent-in-the-world-12107/.

6 International Telecommunications Union, "ICTs facts and figures 2013", ITU Telecommunication Development Bureau (Geneva, 2008). Available from www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013-e.pdf.

7 Goldman Sachs, "eCommerce expected to accelerate globally in 2014", Equity Research, New York: The Goldman Sachs Group, Inc., 5 March 2013. Available from http://boletines.prisadigital.com/Global_ecommerce.pdf.

8 eMarketer, "eMarketer in review – key 2013 trends, coverage areas and platform growth", Newsroom, 4 September 2013. Available from www.emarketer.com/newsroom/index.php/emarketer-review-key-2013-trends-coverage-areas-platform-growth/#UG1Ch9mS5hMlp1JX.99.

poses its own vulnerabilities and risks. One such risk that derives from increased technological exposures and requires urgent policy attention and action is cybercrime.[9]

Cybercrime is a growing global phenomenon, which, according to a report by Symantec, Corporation[10] issued in 2013, is increasing at a more rapid rate in Africa than in any other area of the world. Indeed, cybersecurity experts estimate that 80 per cent of personal computers on the African continent are infected with viruses and other malicious software.[11]

Cybercriminals have long considered Africa as opportune to commit their criminal acts. Statistics from various sources indicate that Africa is very prone to cyber-related threats due to the high number of domains coupled with very weak network and information security. For example, according to the Norton Cyber-Crime Report, every second, 18 adults are victims of cybercrime, resulting in more than 1.5 million victims globally per day. In addition, South Africa (80 per cent) has the third highest number of cybercrime victims in the world, after Russia (92 percent) and China (84 percent).[12]

The Symantec report[10] further reveals that in 2012, the number of targeted cyberattacks in Africa increased by 42 per cent. Thirty-one percent of these attacks, categorized as cyberespionage, have hit both large and small businesses. Individual consumers have also become vulnerable to viruses and other forms of cyberthreats. In Africa, Nigeria is the largest target and source of malicious Internet activities, the consequences of which are unfortunately spilling into the other countries in the West African subregion. In major African cities, such as Cairo, Johannesburg, Lagos and Nairobi, the rate of cyberconnected disturbances, such as fraudulent financial transactions and child kidnappings, especially in Kenya, facilitated through Internet communications has doubled in the past three years.

Recent use of information and communications technologies (ICTs) in support of terrorism attacks throughout Africa is adding an additional dimension to the cybersecurity issue. Evidence from the investigation into the recent attack of the Westgate Mall in Kenya, the activities of Boko Haram in Nigeria and Al-Qaida in Islamic Maghreb (AQIM) in Northern Africa highlight the use ICTs in the planning, coordination, implementation and promotion of the various attacks. Such attacks have destabilized and hampered recent economic growth performances of African countries. For example, the Westgate Mall attack not only cost at least 67 innocent lives and millions of dollars in infrastructure damage, but it is also expected to have cost the Kenyan economy some $200 million in lost tourism revenue.[13]

Consequently, African countries need to urgently scale up efforts to combat cybercrimes through a multi-stakeholder approach involving government, industry and civil society organizations.

As per the new strategic focus of ECA on evidence-based policy and analytical research, this policy brief provides options for consideration by member States, within the context of the African Union Convention on Cyberspace Security and Protection of Personal data to stem the threats posed by cybecrime and cybercriminals, to their national economic security.

9 Cybercrime is defined as a broad range of illegal activities committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network.

10 Symantec Corporation, Internet Security Threat Report 2013, 2012 Trends, Volume 18 (April, 2013). Available from www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf.

11 Franz-Stefan Gacy, "Foreign policy: Africa's internet threat", National Public Radio, 29 March 2010. Available from www.npr.org/templates/story/story.php?storyId=125297426.

12 Symantec Corporation, 2012 Norton Cybercrime Report, September 2012.

13 Jacob Kushner, Jacob, "Mall terrorist attack may cost Kenya $200 million in lost tourism earnings", The Associated Press, 1 October 2013. Available from www.ctvnews.ca/mall-terrorist-attack-may-cost-kenya-200-million-in-lost-tourism-earnings-1.1478573.

2. The economic impact of cybersecurity

The economic impact of inadequate cybersecurity is colossal. The Norton Cybercrime Report 2012 indicated that direct financial losses totalled an average of $197 per victim worldwide, while globally a grand $110 billion in direct financial loss was recorded.[14]

A recent study by the International Data Group Connect[15] investigating the state of cyberthreats in various regions of Africa, with particular emphasis on Egypt, Kenya, Nigeria and South Africa, shows that there is a strong correlation between cybersecurity and economic growth.

Africa, traditionally, has a high rate of software piracy. According to a 2011 study,[16] the average rate of software piracy in the region is about 73 per cent, with little change in recent years. In addition to the financial loss — $1.785 billion —, the high level of use of unauthorized software is likely to aggravate the region's virus and malware woes.

The study by the International Data Group Connect estimates that annually, cybercrimes cost the South African economy $573 million, the Nigerian economy $200 million, and the Kenyan economy $36 million.[15]

A 2011 Deloitte Touche survey found that financial institutions in Kenya, Rwanda, Uganda, the United Republic of Tanzania and Zambia had registered losses of up to $245 million due to cyberfraud,[17] a high sum for countries without highly developed banking systems. Several commercial banks in Zambia[18] were robbed of more than $4 million in the first half of 2013 as a result of sophisticated cybercrime collaborations between Zambians and foreigners.

3. Cybersecurity: challenges for Africa

Africa is facing several Internet-related challenges in relation to security risk, intellectual property infringement and protection of personal data. Cybercriminals target people inside and outside their national boundaries and most African governments have neither the technical, nor the financial capacity to target and monitor electronic exchanges deemed sensitive for national security.

These challenges are:

- Low level of security provisions sufficient to prevent and control technological and informational risks.
- Lack of technical know-how in terms of cybersecurity and inability to monitor and defend national networks, making African countries vulnerable to cyberespionage, as well as to incidences of cyberterrorism.
- Inability to develop the necessary cybersecurity legal frameworks to fight cybercrime. A survey of 21 countries conducted by ECA[19] found that while many countries had proposed legislations, the level of deployment of security systems in both the private and the public sectors to combat cyber-crime was low.
- Cyber-security concerns are broader in scope than national security concerns. Yet, few major significant cybersecurity initiatives in Africa have been implemented. As ICTs are hailed as the end-all to the many pressing problems of Africa, cybersecurity is a critical issue that needs to be dealt more comprehensively.
- There is a need to build an information society that respects values, rights and

14 Symantec Corporation, *2012 Norton Cybercrime Report*, September 2012.

15 International Data Group Connect, "Africa 2013: Cyber-crime, hacking and malware", White Paper. Available from www.idgconnect.com/view_abstract/11401/africa-2013-cyber-crime-hacking-malware.

16 Business Software Alliance, Shadow market: 2011 BSA global software piracy study, ninth edition, May 2012. Available from http://globalstudy.bsa.org/2011/downloads/study_pdf/2011_BSA_Piracy_Study-Standard.pdf.

17 Henry Quarshie and Alexander Martin-Odoom, "Fighting Cybercrime in Africa", Computer Science and Engineering, vol. 2, No. 6 (2012), pp. 98-100.

18 Michael Chawe, "Cyber crime costs Zambian banks $4m", Africa Review, 14 June 2013, Available from www.africareview.com/News/Cyber-crime-costs-Zambian-banks--4millio/-/979180/1883006/-/128vr2iz/-/index.html.

19 Benin, Burundi, the Congo, Cote d'Ivoire, the Democratic Republic of the Congo, Egypt, Ethiopia, the Gambia, Ghana, Guinea-Bissau, Kenya, Madagascar, Mali, Mozambique, Niger, Nigeria, Senegal, Sudan, Togo, Uganda and Zambia.

freedoms and guarantees equal access to information, while encouraging the creation of authentic knowledge and that can build confidence and trust in the use of ICTs in Africa.

- Generally limited levels of awareness of ICT-related security issues by stakeholders, such as ICT regulators, law enforcement agencies, the judiciary, information technology professionals and users.

4. Policy recommendations

Measuring the magnitude of challenges posed by lack of adequate cybersecurity is complex. Cybercrime is transnational in nature. Thus, tackling it requires coordinated and focused policies. The plurality of the issues dictates taking into account its multiple dimensions, which are, among others, scientific, technological, economic and financial, political, and sociocultural. The interaction between these dimensions reinforces the complexity of cybesecurity, which is apparent at several levels.

4.1 Policy, legal and regulatory mechanisms

While continental dependence on ICTs is growing, individuals, organizations and countries are becoming highly vulnerable to attacks on information systems and networks, such as hacking, cyberterrorism and cybercrime. Few individuals and organizations are equipped to cope with such attacks. In this regard, the role of governments in dealing with this important phenomenon cannot be overemphasized. The success of any cybersecurity initiative requires the full involvement and support of the political leadership at the very highest level. The role of governments in putting in place the policy, legal and regulatory framework is of paramount importance. Some of these include the following:

4.1.1 Legal framework

Lack of cybersecurity legislation negatively affects business. It is, therefore, essential that effective anti-spam and cybercrime laws and regulations be put in place in order to ensure confidence and trust in the use of the Internet, including carrying out online transactions, by all stakeholders. This should be enhanced by initiating capacity- building among relevant policy stakeholders and creating a framework for local enforcement of cybercrime mitigation.

4.1.2 Harmonization of policy and legal frameworks

Separate but extremely intertwined to the issue above is that of harmonization. Although member States are at varying levels of tackling cybersecurity and establishing policy instruments and legislative frameworks, given the global nature of cybercrime, policy and legal frameworks need to be harmonized.

Cybersecurity is a global good and global and regional actions are required. There is a need to set minimum standards and procedures to enable the continent to operate as one and instil efficiency and effectiveness in its operations. In this regard, the African Union Commission (AUC) and ECA have been spearheading the development of the African union convention on cyber security, which has been undergoing a series of reviews by the regional economic communities and endorsed by the African Union Ordinary Conference in Charge of Communication and Information Technologies in September 2012 in Khartoum and adopted by the African Union Heads of State and Governments Summit in June 2014 in Malabo. Countries will, therefore, be expected to transpose their cybersecurity laws in the framework of the Convention and others can also be guided by it to develop one.

4.1.3 Coordination and cooperation

Cybersecurity transcends all boundaries. Given the global dimension of cybersecurity, it is difficult to fight against cybersecurity breaches at the national level alone. Combatting cybersecurity breaches requires cooperation at all levels, among countries and international organizations, and between the public and private sectors. Thus, a comprehensive framework for international cooperation and outreach must

be developed. To accomplish this, coordination and collaboration in areas including computer-aided fraud, hacking, distribution of child abuse images and copyright infringement, as well as uniformity in procedures and processes, must occur.

4.2 Technological considerations

4.2.1 Development of infrastructure and services

- There should be dedicated national network infrastructures that can connect government, industry and the research community for the benefit of promoting open knowledge engagement, an open data system for researchers, innovation, end-users and researchers' synergy and information technology development.
- There is also a need to establish a national computer emergency readiness and response team ecosystem to promote national synergy on cybersecurity, knowledge-sharing and intelligence gathering on countermeasures against cybercrime injurious to States, as well as to individuals.
- A dedicated call centre for reporting cybecrime should be set up with the aim to assure cybervictims that there is a place that they can turn to report such crimes and receive assistance. As part of the broader cybersecurity strategy, the call centre should be staffed by sufficiently trained and knowledgeable personnel and have a website and a toll free number to enable victims to report a cybecrime with minimal inconvenience.
- The dissemination of best practices of Internet service providers and registrar/registry in their efforts to mitigate cybercrime activities and undertake capacity-building for e-commerce and online transaction providers should be promoted.

4.2.2 Investment on research

Knowledge and information serve as a direct way of empowering countries and their citizens. Currently, there is general lack of knowledge and information on cybersecurity matters in Africa. This gap must be closed. To achieve this, sufficient resources has to be channelled towards investment in research on cybersecurity in Africa, which is currently lacking. Even in cases in which research has been carried out, such material is not readily available and accessible. Thus, databanks need to be created to serve as platforms for researchers to deposit their outputs, including tools and techniques used to identify and gather information about cybercrime activities. Some countries have in place data deposit laws. As these are very useful, those without such laws, should impose them using best practices of countries that have already established them.

4.3 The social dimensions

4.3.1 Education

The exponential growth in the use of cyberspace in Africa is not matched by the necessary skills. Thus, there is a need for broad-based education initiatives on Internet safety and security to tackle the issues of child protection and social security in general. Furthermore, facilitation of secure ICT access for users is of a paramount importance.

4.3.2 Engagement of all key stakeholders

It is important to understand that no one person or institution can have the requisite capacity to deal with cybersecurity. Cybesecurity is not an event but rather a process. As a result, it is not simply a matter of passing legislation, or something that belongs to lawyers only. Members of Parliament, lawyers, the judiciary, intelligence/military, civil society, media, young people and members of the public as key stakeholders should all be involved in efforts to deal with cybersecurity at the earliest

available opportunity. It is important to engage all stakeholders to ensure the necessary buy-in and that they understand the issues and processes involved.

References

Atta-Asamoah, Andrews. (Jul 2010). Understanding the West African cyber-crime process. African Security Review Vol. 18 No.4 pp.105-114. Institute for Security Studies. http://www.tandfonline.com/doi/s/10.1080/10246029.2009.9627562?journalCode=rasr20#.Uu9NOPtdx8E.

Kaiko Namusa,Cyber crime costs banks $4m. Times of Zambia. http://www.times.co.zm/?p=18423 Cyber-crime-costs-Zambian-banks--4millio/-/979180/1883006/-/128vr2iz/-/index.html

United Nations Office on Drugs and Crime (February 2013) Comprehensive Study on Cybercrime. http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_ STUDY_210213.pdf

This policy brief was contributed by Mr. Mactar Seck with support from Ms. Tsega Belai under the supervision of Mr. Kasirim Nwuke, Chief, NTIS

Contact

Further information on ECA's programme on Technology and Innovation can be obtained from Mr. Kasirim Nwuke, Chief, New Technologies and Innovation Section/Special Initiatives Division, Telephone: +251-11-544-3375, Office Fax: +251-11- 551-0512, email: Knwuke@uneca.org.

Ordering information

To order copies of *Tackling the challenges of cyber-security in Africa* policy brief by Economic Commission for Africa;

Please contact

Please contact: Publications, Economic Commission for Africa, P.O. Box 3001, Addis Ababa, Ethiopia, Tel: +251 11 544-9900, Fax: +251 11 551-4416, E-mail: ecainfo@uneca.org

Web: www.uneca.org