ONLINE *in* africa

"Our leaders need a reorientation, not tomorrow but today."

– TIM AKANO, CEO, New Horizons Nigeria[1]

By DR. ERIC YOUNG, Marshall Center

The rising popularity of computers and mobile phones demands greater Internet protection

As the e-revolution sweeps across Africa, cyber security has become a major emerging challenge. The continent's significant Internet-penetration growth rates are challenging the notion of a global digital divide. Economies are growing, social structures are changing, and political systems are transforming. Maasai ranchers can check cattle market prices on their mobile phones, and Africa's new high-speed undersea cables are leading an entrepreneurial boom in Kenya and Ghana. Rwanda's Vision 2020 is a youth-led, knowledge-based economy, and the Nigerian government recently launched a "Single Window Trade Portal" to facilitate trade and standardize services. However, with dramatic growth and change come challenges and threats to security from cyber crime, intellectual property theft, espionage and cyber attacks. To ensure that Africa fully benefits from the e-revolution, the continent's governments must take cyber security seriously, and nations worldwide can learn from Africa's approach.

Bedouins use a laptop computer in the Sahara in Tunisia. Mobile Internet use in Africa is among the highest in the world.

AGENCE FRANCE-PRESSE

AFRICA'S E-REVOLUTION

In the past few years, 11 new undersea fiber-optic cable systems surrounding Africa were completed, thanks to international and local investment.[2] This has brought faster and cheaper broadband connectivity to the continent. Economic growth, urbanization and a rapidly growing youth population have followed and created new economic opportunities. Cyber cafes have opened in war-torn Somalia; engineers in Kenya, Rwanda and South Africa are building new software for worldwide markets; and e-commerce is taking off from Algeria to Zimbabwe.

The numbers are impressive: Six out of the world's 10 fastest growing economies are in Sub-Saharan Africa, which has contributed to the creation of the second largest mobile phone market in the world. Smartphones outsell computers 4 to 1 in Africa, and it is estimated that Africa will have 1 billion mobile phones by 2016. Mobile Internet usage is among the highest in the world, and annual growth in the use of social media exceeds 150 percent.[3] There are more than 90 tech hubs, innovation labs, and e-incubators in more than 20 African countries. In addition to the economic and social impact, the political impact has been profound. The software platform, Ushahidi, emerged from and shaped the post-electoral violence in Kenya in 2008, @GhanaDecides educated voters prior to the 2012 elections, and social media had a profound role in the Arab Spring throughout North Africa in 2010.

Africa's e-revolution has not been without its challenges. Access to broadband remains uneven, focused mostly on the Anglophone countries and coastal urban hubs. Africa remains a "dumping ground" for second-hand, second-generation mobile devices and personal computers that are more vulnerable to attack and likely already to contain malicious code. An estimated 80 percent of the personal computers in Africa are already infected with viruses and other malicious software.[4] Mobile phone service has been used by some to advocate violence, and states have used it to limit freedoms and human rights. Yet on balance, all facets of life in Africa, from food security to health care access, employment opportunities to democratic freedoms, have benefited from the e-revolution.

THREATS TO AFRICA

To date, Africa has experienced a honeymoon in cyberspace. Most cyber attacks have been relatively unsophisticated with little impact. Cyber crime, off-the-shelf malware, phishing, or email-based advance-fee scams (commonly known as Nigerian 419 scams or in Nigeria as *yahoo-yahoo*) are referred to as *bafere* by Ugandans, and Ghanaians call it *sakawa*. Average citizens are routinely victims of cyber attacks, and only recently have cyber attacks had a major economic impact. The availability of more affordable Internet service and the increase of e-commerce have led to a rise in cyber crime. Likewise, the substantial growth in cellular telecommunications has led to more cyber attacks on smartphones. In 2012, South Africa, the most advanced e-commerce market on the continent, also ranked as the world's second most targeted country for phishing attacks. In October 2013, a variant of the "Dexter" malware program cost South African banks millions of dollars when it was inserted into point-of-sale devices at fast-food chains. In Nigeria, from 2010 to 2012 there was a 60 percent increase in attacks against government websites, which included attacks against the Central Bank of Nigeria, the Ministry of Science and Technology, and the Economic and Financial Crimes Commission.[5]

REUTERS

Workers lay fiber optic cables near the coastal city of Mombasa, Kenya, in June 2009. Eleven undersea fiber-optic cables have been laid in Africa in the last few years, providing faster and more affordable Internet connections.

Much more opaque and difficult to quantify is the theft of intellectual property (IP), cyber espionage, the costs of cyber security, and opportunity and reputational costs associated with malicious cyber activities. As McAfee and the Center for Strategic and International Studies note, the economic impact of the theft of IP is probably several times more than the cost of cyber crime.[6] Africa is not a leader in IP, yet as the e-revolution sweeps the continent, there will be more IP emerging from Africa and the theft of IP and sensitive business information is likely to increase. And although Africa, except for South Africa, is currently not a major target of cyber espionage, the threat is real.[7]

So, too, is the likelihood that some states will develop offensive cyber capabilities, further skewing the military capabilities between the "haves" and "have-nots." Information is not available on whether an African state or nonstate actor has successfully conducted an offensive cyber attack, but the social media and online presence of terrorist groups such as al-Shabab in Somalia demonstrates the ease and cost-effectiveness of such an attack. And because cyber crime is a transnational issue, African countries and their citizens remain vulnerable to attacks from anywhere in the world.

LAYERS OF SOLUTIONS

Africa faces many cyber challenges. First, African governments have limited capabilities in writing legislation and enforcement. In Kenya, for instance, fewer than 50 percent of cyber crimes are successfully investigated to the point of achieving a conviction.[8] Governments have only begun to fund cyber security, and governments lack information technology (IT) and cyber security professionals. Laws and regulations covering mobile telephones and Internet service providers (ISPs) are in their infancy, and enforcement is often lax. Corruption is endemic and spills over into the cyber domain. At the same time, the United States and Europe do not offer particularly good examples to follow, because they are heavily dependent on the private IT security industry and often behind the curve when it comes to cyber crime. Internationally, there isn't a central repository of cyber knowledge, expertise or training where Africa-specific solutions are presented.

Several "layers" of solutions to these challenges have emerged in Africa, from increasing cyber awareness to establishing Computer Emergency Response Teams (CERTs). National strategies against cyber security and international collaboration are necessary to ensure the e-revolution continues in Africa.

Cyber awareness through education and training is vital. This includes public and corporate awareness but most importantly awareness among lawmakers about the threats and opportunities of cyber security issues. Some in government have recognized the need for public awareness. As noted by Dr. Bitange Ndemo, Kenya's permanent secretary of the Ministry of Information and Communication: "The new government's pledge to provide a laptop to every child presents an opportunity for creating cyber security awareness at an early age. …

This will lead to a new generation of technology savvy people who are conscious about the effects of cybercrime."[9] Growing awareness will lead to growing demand for cyber security in Africa, and cyber security companies and ISPs must also facilitate protection. For instance, credit cards are widely required for online software purchases, yet credit cards are luxuries many Africans do not possess. Government should work with ISPs to provide greater public and private security.

In addition to increasing awareness, national cyber capacity is key. Further government training of experts as well as policy, legal and regulatory reforms will be needed to prevent and respond to cyber security threats and incidents. Several countries have quickly hired an impressive number of cyber human-resources staff, but only South Africa and Egypt have a significant number of trained cyber security experts. In recent years, a few countries have passed laws related to cyber security, cyber crime and data protection, but many already need updating, while other countries are struggling to catch up.[10] To better control crimes committed with the use of a mobile phone, SIM card registration is increasingly a requirement. Expertise in the cyber domain is needed at all levels across the government. A positive step would be to bolster law enforcement. Ghana, South Africa and Uganda have created new cyber units within their police forces.

The creation of national CERTs indicates growing government awareness and capacity. Eleven African countries have established them,[11] and a continentwide AfricaCERT based in Ghana coordinates incident reporting and promotes cyber security education and human resource development. Some CERTs have been impressive. In 2012, the new CERT in Côte d'Ivoire investigated 1,892 incident reports and authorities made 71 arrests, leading to 51 convictions on cyber security-related crimes.[12] Yet CERTs are also evolving institutions that must themselves learn to cooperate with other CERTs and the rest of government to be fully operational.

CERTs are only part of a comprehensive national cyber security strategy. Indeed, it can be a vital tool to ensure that scarce government resources are being appropriated to the cyber realm. South Africa emerged as a leader in cyber strategy on the continent, developing a national cyber security strategy in 2010 and inaugurating a National Cyber Security Advisory Council in 2013. Uganda also has a national cyber security strategy, and Kenya is developing a national cyber security master plan. In national strategies, it is important, as the South African and Ugandan strategies demonstrate, to take a whole-of-government approach, which ensures that the strategy is effective and will build national cyber capability, not just the power of one ministry or the capabilities of the government.

In addition to national strategies, regional and international approaches have improved cyber security in Africa. Regional economic communities have sought to collaborate on cyber security — the most active being the Southern Africa Development Community and the East African Community. For the past four years, the African Union has been considering an African Union Convention on Cyber Security that includes sections on electronic commerce, personal data protection and cyber crime with a special focus on racism, xenophobia and child pornography. But the draft convention has not been well-received among defense ministries in Africa. Critics are concerned the convention would curb Internet freedom. At the same time, leaving cyber security to the private sector in Africa is not a feasible, because profit-seeking, corruption and a weak legal framework do not correlate with national security requirements. Academia, think tanks and nongovernmental organizations will undoubtedly play important roles but they lack the financial resources to take the lead.

CONCLUSIONS

Africa's e-revolution will continue. Many Africans benefit from increased global connectivity. Africa's emerging cyber entrepreneurs must be embraced, both by the global community and by their governments. Uniquely African approaches, research and solutions are important for any cyber security strategy to take hold. But this growth, and indeed Africa's economic growth in general, will depend on improving cyber security. Continued prosperity in Africa will help pay the high costs of cyber security. Cyber security is not something that governments should simply outsource to the private sector or nongovernmental organizations. Countries must form partnerships, share best practices, build technical capabilities and offer legal guidance to one another. When it comes to cyberspace, everyone will sink or swim together. □

1. As quoted in Cristina Gallardo, "African Union Set to Get Tougher on Cybercrime," Allafrica.com, December 30, 2013, available at http://allafrica.com/stories/201312301604.html?aa_source=sptlgt-grid
2. For a summary, see Lucif Kharouri, "Africa: A New Safe Haven for Cybercriminals?" Trend Micro Research paper, 2013, pp. 3-4. Available at http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-ice-419.pdf
3. Jonathan Kalan, "African youth hungry for connectivity," *AfricaRenewal,* May 2013. See more at: http://www.un.org/africarenewal/magazine/may-2013/african-youth-hungry-connectivity#sthash.rIejOhul.dpuf
4. B. Rowe, D. Reeves, D. Wood and F. Braun, "The Role of Internet Service Providers in Cyber Security," Institute for Homeland Security Solutions, June 2011, at http://sites.duke.edu/ihss/files/2011/12/ISP-Provided_Security-Research-Brief_Rowe.pdf
5. "Cyber Attacks At Nigerian Government Websites Increased By 60% In 2012," TechLoy, January 17, 2013. Available at http://techloy.com/2013/01/17/nigerian-government-websites-cyber-attack-report/
6. McAfee, "The Economic Impact of Cybercrime and Cyberespionage," McAfee Report, July 2013.
7. South Africa appears to have been the only target of the suspected Chinese People's Liberation Army Unit 61398 offensive cyber group. See Mandiant Intelligence Center Report, "APT1: Exposing One of China's Cyber Espionage Units," February 2013, p. 22. Available at http://intelreport.mandiant.com/
8. "Roundup: African governments seek to collaborate on cyber security," *Global Times,* May 28, 2013, available at http://www.globaltimes.cn/content/784802.shtml
9. Ibid.
10. See Kharouri, "Africa: A New Safe Haven," p. 8.
11. These include Burkina Faso, Cameroon, Côte d'Ivoire, Egypt, Ghana, Kenya, Mauritius, Morocco, South Africa, Sudan and Tunisia. Burundi and Uganda are in the process of creating national CERTs.
12. Rebecaa Wanjiku, "Africa Increases Cybersecurity Efforts," IT World, June 21, 2013 available at http://www.itworld.com/security/362093/africa-increases-cybersecurity-efforts