Institute for Security Studies
POLICY BRIEF

RECOMMENDATIONS

African countries should:

- Adopt a universal definition of cybercrime, which must be included in national cybercrime laws.
- Strengthen international and regional collaboration to counter cybercrime.
- Designate a civilian rather than a military government agency to lead governmental response to cybercrime.
- Develop domestic criminal justice capacity to understand cybersecurity and respond appropriately to threats.
- Create cyber emergency response teams with 24/7 capabilities to respond to significant threats and provide technical assistance.
- Establish a cybercrime coordination hub and watch centre to enhance real-time sharing of cyber threat information.
- Promote research and development to spur technological innovations to defend against evolving cybercrime techniques.
- Develop educational programmes that teach technical skills to combat cybercrime.
- Implement public cyber awareness campaigns to educate those targeted by cybercrime to better protect themselves.

Cybercrime

A complex problem requiring a multi-faceted response

Eric Tamarkin

SUMMARY

The Internet has revolutionised the way in which businesses, government and the public interact. However, criminal actors have used this to their advantage. Given reports that Africa is becoming a cybercrime safe harbour, this problem could hamper economic growth, foreign investment and security. African policymakers need a cogent response to cybercrime, which is informed by a clear understanding of emerging threats and how other countries have formed strategies in response.

In the absence of a universal definition of cybercrime, the term is often confused with other types of malevolent cyber activity and it is difficult to quantify its financial impact worldwide. A recent study estimated the cost of malicious cyber activity to the global economy to be as high as US$1 trillion. Recent high-profile cyber attacks and emerging threats such as attacks on mobile technologies demonstrate that cybercrime is an urgent issue for policymakers. In devising a strategy to combat cybercrime, countries on the continent should adopt a multi-layered approach.

A GROWING CONCERN

The growth of the Internet has been astounding. According to the International Telecommunication Union (ITU), over 2.7 billion people had Internet access in 2013, which corresponds to almost 40 per cent of the world's population.[1] There were over 167 million Internet users in Africa as of mid-2012, with Nigeria's more than 48 million Internet users representing the largest portion.[2] Given that over 60 per cent of Internet users are in developing countries and 45 per cent are below the age of 25,[3] Internet penetration will grow exponentially around the world and particularly in Africa.

To keep up with the increasing demand for connectivity, governments and the private sector have collaborated to expand the information and communication technology (ICT) infrastructure. In 2007, SEACOM built Africa's first undersea fibre-optic cable infrastructure. Since then, several other cable projects have linked most of the continent to the global Internet infrastructure. As a result, African Internet service providers are now able to deliver cheaper and faster access.

While the Internet provides many benefits, it also provides new opportunities for criminals. If African policymakers fail to address this threat, there will be negative impacts on economic growth, foreign investment and security. In order to stem the cybercrime explosion, African policymakers need to understand the definition of cybercrime; its impact; emerging threats and how other countries have responded.

DEFINING CYBERCRIME AND QUANTIFYING ITS GLOBAL IMPACTS

There is no universally accepted definition of cybercrime. The term is often used when a computer or related technology has been utilised in a crime. Cybercrimes can also be viewed as digital versions of 'traditional' offences, such as distributing illicit drugs or sex trafficking. The website Silk Road, for example, facilitated US$1.2 billion in drug deals and other crimes before United States authorities shut it down.[4]

Cybercriminals also use the Internet to commit crimes such as hacking, 'phishing' (where users are tricked into installing malicious software or giving away information) and illegal data interception.

The African Union's (AU's) draft convention on cybersecurity, which was removed from the agenda of the January 2014 summit, identifies four categories of cybercrime: attacks on computer systems (e.g. fraudulently accessing a computer system); attacks on computerised data (e.g. fraudulently intercepting data); content-related offences (e.g. disseminating child pornography); and offences relating to electronic message security measures.[5] The Council of Europe's Cybercrime Treaty also designates four broad categories of cybercrime: offences against computer data and systems (e.g. hacking); computer-related forgery and fraud (e.g. phishing); content offences (e.g. disseminating child pornography); and copyright offences (e.g. disseminating pirated content).[6]

Cybercrime should be distinguished from cyber espionage, cyber warfare, cyber terrorism, and cyber 'hacktivism'. In order to properly classify a cyber attack, the motivation of the attacker should be determined.

Actors engaged in cyber espionage seek access to intellectual property or secure information for political, military or business strategic advantage. Those engaged in cyber warfare intend to sabotage, disrupt or inflict physical damage on an enemy's critical infrastructure. A cyber terrorist also uses cyber attacks to target critical infrastructure, but intends to intimidate the civilian population to further political, religious or ideological goals.[7]

There is an ongoing debate about the definition of cyber hacktivism. Some argue that these actors effect social change, while others claim that cyber hacktivists are malicious actors who ought to be prosecuted accordingly.[8]

In contrast to those who engage in other types of cyber attacks, cybercriminals generally seek monetary profit. Governments should agree on a clear definition so that statistics can be gathered, strategies developed and resources spent on cybersecurity can be used efficiently.

The difficulty in obtaining comprehensive data on cybercrime is exacerbated by the reluctance of companies and individuals to disclose that they were victims of cyber attacks. While it might be embarrassing for individuals to report being victimised by cybercriminals, companies could suffer devastating financial and reputational harm. Additionally, global cybercrime statistics often include factors that could inflate monetary impacts beyond the direct financial losses resulting from cybercrime.

Despite these barriers and caveats, several entities have attempted to gather and report global statistics. Symantec Corporation, a data security and antivirus provider, has estimated the total global direct cost of cybercrime to be US$113 billion in 2013 (up from US$110 billion in 2012) and the average cost per victim of cybercrime to be US$298 (up from US$197 in 2012).[9] A recent study by McAfee, another data security and antivirus provider, found an estimated cost of malicious cyber activity to be US$300 billion to US$1 trillion for the global economy. McAfee included components such as the loss of intellectual property, opportunity costs and reputational damage.[10]

Recent high-profile incidents also confirm that cybercrime is a growing transnational problem. For example, a European-based criminal syndicate reportedly utilised the Dexter malware to attack a wide range of South African retailers and steal tens of millions of rands.[11] In another prominent case, a multinational group of cybercriminals allegedly infiltrated debit card accounts from the National Bank of Ras Al-Khaimah in the United Arab Emirates and Bank Muscat in Oman. The cybercriminals created fraudulent debit cards that were used in more than 20 countries to withdraw US$45 million.[12]

ATTACKS ON MOBILE DEVICES

In Africa, an emerging threat that is particularly salient is the increasing vulnerability of mobile devices such as smartphones and tablets. As more people in Africa rely on mobile technologies, cybercriminals are developing their strategies to exploit cybersecurity gaps.

The use of mobile devices is growing at an astonishing rate. By 2017, 70 per cent of the world's population will have mobile broadband subscriptions; by 2020, the number of networked devices will outnumber people by six to one.[13]

According to the Groupe Spéciale Mobile Association (GSMA), sub-Saharan Africa has been the world's fastest growing mobile market for the past five years and is predicted to continue that trend. As of mid-2013, sub-Saharan Africa had 253 million unique mobile subscribers; set to increase to 346 million by 2017.[14] Additionally, Africa's smartphone market is expected to double by 2017.

South Africa currently has sub-Saharan Africa's largest smartphone market, with 19 per cent penetration, with the markets in Tanzania, Nigeria and Kenya closely behind.[15]

Many in Africa rely on mobile devices to conduct financial transactions. In Kenya, over 17 million people use M-Pesa, a mobile-phone-based money service[16] that allows people to deposit, withdraw and transfer money.[17] Other new mobile banking technologies are also emerging in a rapidly evolving landscape.

The mobile platform is also a fertile ground for Nigerian advance-fee fraud, which involves a fraudster who usually communicates by SMS, phone or email and tricks the victims into sharing banking details and other information.

Mobile devices typically lack protections such as firewalls, antivirus software and encryption.[18] Thus mobile users are more vulnerable to software exploits, such as applications that capture information and passwords.

COMBATTING CYBERCRIME: A MULTI-FACETED APPROACH

In recognition of the growing cybercrime threat,[19] some countries have developed multi-faceted responses that involve government, citizens and the private sector.

A cogent response begins with policy frameworks that clearly allocate roles to particular governmental agencies and departments. In South Africa, the Cabinet approved the Cyber Security Policy Framework on 11 March 2012, which tasks the State Security Agency with the responsibility for the coordination, development and implementation of cybersecurity measures.

In the US, the Department of Homeland Security (DHS) is responsible for securing civilian government networks, while the Department of Defence is responsible for securing military networks and gathering foreign cyber threat information. The Department of Justice (DOJ), a civilian law enforcement agency, spearheads efforts to counter cybercrime. Acting with its law enforcement components such as the Federal Bureau of Investigation (FBI), the DOJ investigates cybercriminals, seizes their hardware and assets and deters cybercrime through arrest, prosecution and appropriate punishment.[20] The DOJ closely collaborates with other agency stakeholders.

To facilitate interagency collaboration and enhance the sharing of cyber threat information in real time, it is essential to have 24/7 cyber watch centres. In Kenya, the Kenya Computer Incident Response Team Coordination Centre (KE-CIRT/CC) coordinates and manages responses to cybersecurity incidents nationally, and collaborates with relevant actors locally, regionally and internationally.

While South Africa does not yet have a government-sponsored watch centre, banks have funded the South African Banking Risk Information Centre (SABRIC), which tracks and responds to cybercrime targeting the banking sector. SABRIC coordinates closely with the South African Police Service (SAPS), the Directorate for Priority Crime Investigation ('the Hawks') and the Special Investigating Unit's Cyber Forensic Laboratory.

Computer Emergency Readiness Teams (CERTs) or Computer Security Incident Response Team (CSIRTs) are also essential to respond to cyber incidents, provide technical assistance to hacked entities and disseminate notifications regarding threats. The following countries in Africa have CERTs or CSIRTs: Botswana, Burkina Faso, Côte d'Ivoire, Egypt, Ghana, Kenya, Mauritius, Morocco, South Africa, South Sudan and Tunisia.[21]

AfricaCERT, which is based in Ghana, serves as a forum for these teams to coordinate responses as well as to share technical information, tools and best practices.

To keep up with evolving threats, law enforcement agencies, prosecutors and public sector cyber professionals must receive training on current cybercrime trends and techniques. In Ghana, for example, the e-Crime Bureau routinely trains government, law enforcement and intelligence officials on ways to counter emerging threats.

Formal training can be augmented by establishing a cybersecurity curriculum in the education system. The University of Johannesburg has partnered with the Academy of Computer Science and Software Engineering to create the Centre of Excellence in Cyber Security; the first such facility in Africa, dedicated to fighting cybercrime.

Raising public awareness is also critical. In South Africa, the Wireless Access Providers' Association and others led the Internet Security Campaign Africa 2013. The Council for Scientific and Industrial Research (CSIR) and various universities have also developed campaigns.

In countries where no legislation is in place to regulate cybercrimes, it is imperative that such legislation is adopted. According to the Global Centre for Information and Communication Technologies in Parliament, only five African countries have enacted cybercrime laws.[22] These are Cameroon, Kenya, Mauritius, South Africa and Zambia. Several other African countries, including Nigeria, are in the process of developing cybercrime laws.[23]

While these laws should address each country's unique challenges, they should also be harmonised with those of other countries. The Council of Europe Convention on Cybercrime seeks to do just that. It is the first international treaty on cybercrime and its primary purpose is for nations to adopt a common approach to legislation and enhance international cooperation. The Convention has been ratified by 41 countries and signed by 11 others.[24]

South Africa is the only African country that has signed the Convention. The AU has also proposed such a convention. Awaiting a formal vote, this convention seeks to define cyber terminologies, outline legislative measures and harmonise cyber legislation and provisions.[25]

Additionally, research and development (R&D) is integral to informing an effective response to cybercrime. Entities such as the DHS Science and Technology Directorate Cybersecurity Division work with private sector partners to 'develop … new technologies, tools, and techniques to protect and secure systems … infrastructure and users.'[26] In South Africa, the CSIR leads cybersecurity R&D.

As many in Africa work to prevent conventional crimes, they may lose sight of their growing vulnerability in the virtual world. Based on the staggering global financial impact statistics and recent high-profile cybercrime incidents, failure to address cybercrime can have dramatic consequences. While there is no silver bullet to prevent cybercrime, governments can begin to respond effectively if they pursue a multi-layered, collaborative approach.

ABOUT THE AUTHOR

Eric Tamarkin is a research consultant at the ISS and previously served as a Senior Counsel for the United States Senate Homeland Security & Governmental Affairs Committee, where he specialised in cybersecurity policy.
The author would like to thank Anton du Plessis and Ottilia Maunganidze for their guidance and insight.

NOTES

1 International Telecommunication Union, The World in 2013: ICT facts and figures, www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013.pdf (accessed November 2013).

2 Internet World Stats, Internet Usage Statistics for Africa, www.internetworldstats.com/stats1.htm (accessed November 2013).
3 UN Office on Drugs and Crime, Comprehensive Study on Cybercrime, February 2013, www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (accessed November 2013).
4 Nick Bilton, Disruptions: A Digital Underworld Cloaked in Anonymity, *The New York Times*, 17 November 2013, bits.blogs.nytimes.com/2013/11/17/disruptions-a-digital-underworld-cloaked-in-anonymity/?r=0 (accessed November 2013).
5 Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa, 1 September 2012, au.int/en/cyberlegislation (accessed November 2013).
6 Council of Europe Convention on Cybercrime, conventions.coe.int/Treaty/en/Treaties/Html/185.htm (accessed November 2013).
7 William L Tafoya, Cyber Terror, November 2011, www.fbi.gov/stats-services/publications/law-enforcement-bulletin/november-2011/cyber-terror (accessed November 2013).
8 Peter Ludlow, What Is a 'Hacktivist'?, *The New York Times*, 13 January 2013, opinionator.blogs.nytimes.com/2013/01/13/what-is-a-hacktivist (accessed November 2013).
9 Symantec, Norton Cybercrime Report 2013, 1 October 2013, www.symantec.com/about/news/release/article.jsp?prid=20131001_01 (accessed November 2013).
10 McAfee, The Economic Impact of Cybercrime and Cyber Espionage, July 2013, www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf (accessed November 2013).
11 Leo Kelion, Dexter Payment Card Malware Strikes South Africa, BBC News, 16 October 2013, www.bbc.co.uk/news/technology-24550505 (accessed November 2013).
12 Bernard Vaughan, Six Arrested in $45 Million Global Cybercrime Scheme, Reuters, 18 November 2013, uk.reuters.com/article/2013/11/18/uk-usa-crime-cybercrime-idUKBRE9AH0Z020131118?feedType=RSS&feedName=topNews (accessed November 2013).
13 UN Office on Drugs and Crime, Comprehensive Study on Cybercrime, February 2013, www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (accessed November 2013).
14 GSMA, Sub-Saharan Africa Mobile Economy 2013, November 2013, www.gsmamobileeconomyafrica.com/Sub-Saharan%20Africa_ME_Report_English_2013.pdf (accessed November 2013).
15 Nmachi Jidenma, The Real Mobile Revolution: Africa's Smartphone Future, CNN, 7 November 2013, edition.cnn.com/2013/11/07/opinion/real-mobile-revolution-africa-smartphone/index.html (accessed November 2013).
16 Why does Kenya lead the world in mobile money?, *The Economist*, 27 May 2013, www.economist.com/blogs/economist-explains/2013/05/economist-explains-18 (accessed November 2013).
17 Ibid.
18 Ibid.
19 The Director of the Federal Bureau of Investigation, James B Comey, recently testified before the US Senate that he expected Internet-related attacks, espionage and theft to emerge as the top threat to the US.
20 US Senate Committee on the Judiciary, Subcommittee on Crime and Terrorism, Hearing on Cyber Threats: Law Enforcement and Private Sector Responses, testimony of US Attorney Jenny Durkan, Department of Justice, 8 May 2013, www.judiciary.senate.gov/pdf/5-8-13DurkanTestimony.pdf (accessed November 2013).
21 AfricaCert, www.africacert.org (accessed January 2014).
22 The Global Centre for Information and Communication Technologies in Parliament, Legislative Acts on ICT – Cybercrime, www.ictparliament.org/legislationlibrary/Cybercrime (accessed January 2014).
23 Business Day, FG approves cybercrime bill, N32bn credit facility for FADAMA 111, *Business Day*, businessdayonline.com/2013/08/fg-approves-cybercrime-bill-n32bn-credit-facility-for-fadama-111/ (accessed January 2014).
24 Council of Europe Convention on Cybercrime, Treaty Office, conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG (accessed November 2013).
25 Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa, 1 September 2012, au.int/en/cyberlegislation (accessed November 2013).
26 US Department of Homeland Security, Science and Technology Directorate Cyber Security Division, www.dhs.gov/science-and-technology-directorate-cyber-security-division (accessed November 2013).

The work of the ISS is made possible with the support from the following core partners: the governments of Norway, Sweden, Australia and Denmark.

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

ISS Nairobi
Braeside Gardens,
off Muthangari Road,
Lavington, Nairobi,
Kenya
Tel: +254 20 266 7208
Fax: +254 20 266 7198
Email: nairobi@issafrica.org