PARTICIPANTS' PAPERS

THE STATE OF CYBERCRIME: CURRENT ISSUES AND COUNTERMEASURES

*Joash Dache, MBS**

I. INTRODUCTION

That the world has seen remarkable transformation with the advent of internet-based activities cannot be overemphasized[1]. This is because goods and services are routinely purchased and delivered electronically, leading to significant changes in various industries like journalism, travel, and banking. Significantly, a majority of the people, especially in developed and the elite in developing economies, relies on the Internet, either directly or indirectly, for most services. What is interesting is that this trend is not expected to slow down soon especially with ever increasing globalization[2]. Concomitant to this phenomenal growth of the Internet is the fact that it has occasioned a number of challenges most of which revolve around its universal and trans-territorial character allowing direct, instantaneous and multifaceted exchange of information among literally tens of millions of users over global computer networks. This trans-nationally dominant and free nature of the Internet was the conventional wisdom in the 1990s[3].

A number of legal principles have been tested in the courts as a result of this global reach of the Internet. In the Australian case of *Dow Jones & Company Inc. v Gutnick*[4] for example, the High Court of Australia asserted jurisdiction in proceedings relating to online defamation where the alleged defamatory material uploaded on the Internet in New Jersey, United States, was downloaded in Victoria by subscribers to an online business news service. The Court held that publication of the defamatory material had occurred in Victoria where the material was accessed by subscribers.

As already seen above, the Internet has revolutionized local and global communication given its transnational and ubiquitous nature. A combination of these features and the anonymity embedded in its use has made the Internet an attractive tool for those with propensity to engage in unlawful acts. This presents significant challenges to governments and law enforcement agencies in regulating online activities[5]. It is feared that should current trends continue, the perception by users that the Internet is unsafe and therefore unsuitable for everyday use may become widespread and eventually lead to a loss of faith in "the system"[6]. It is believed that cybercrime, and other cyber-issues are the one area that could cause this type of loss of faith in the safety of the Internet.

II. CURRENT TYPES OF CYBERCRIME

Cybercrime, not unlike other forms of crime, is a multi-faceted and ever-changing problem. The conventional definition relates it to crime that involves a computer and a network. Ordinarily, the computer may be a platform for the commission of a crime or it may be the target. In its broader sense cybercrime boils down to criminal exploitation of the Internet. Attendant unlawful activities around this type of crime

*Secretary/CEO, Kenya Law Reform Commission, Kenya.

1 See generally, Brian Fitzgerald et al, '*Internet and E-Commerce Law: Technology Law and Policy*' (Lawbook Co, Sydney, 2007).

2 See generally Claude Barfield et al. (eds), *''Internet, Economic Growth and Globalization' Perspectives on the New Economy in Europe, Japan and the USA* (Springer-Verleg, Berlin 2003); and Jack Goldsmith and Tim Wu, *'Who Controls the Internet? Illusions of a Borderless World'* (Oxford University Press, Oxford, 2006) 79-81.

3 See, e.g., John Perry Barlow, *'A declaration of the Independence of Cyberspace'* (1996) <http://homes.eff.org/~barlow/Declaration-Final.html>at 12 April 2008.

4 (2002) 210 CLR 575; (2002) 194 ALR 433; (2002) HCA 56.

5 See, e.g., Fitzgerald, above n 2,691-2.

6 Michael Barrett, et al. "Combating Cybercrime: Principles, Policies, and Programs" April 2011 <www.paypal-media.com/assets/pdf/fact_sheet/... > 5 May 2015.

include: computer hacking, copyright infringement, identity theft, child pornography and child grooming[7].

In conversations on activities of government and non-state actors alike, one ordinarily comes across related variants of cybercrime such as cyberespionage, cyberwarfare and cyberterrorism. Cyberespionage refers to the process of hacking into computer systems in order to steal information, especially if the information is deemed to be of commercial value. A common example of this is 'industrial espionage' which occurs when unscrupulous companies spy on competitors and even on individuals[8].

Cyberterrorism on the other hand is evidenced by attacks against one or more parts of the Internet with the aim of precluding legitimate users from being able to use internet-based services, to instill fear that the integrity of services has been compromised, and most importantly to cause fear in the power of the group behind the attack[9]. It has been explained that the difference between cyberterrorism and cyberwarfare lies in three aspects: intention, scale, and actor. As such the intention in a full-scale cyberwar is to cripple the target (be it the economy, communications or essential services), or to create confusion prior to or during an actual attack. In these situations, direct control by the state or close collaboration of the state with these actors cannot be ruled out[10].

A number of cyberthreats have recently been identified. These comprise:

(a). Malicious Code: This includes any 'hardware, software or firmware' that is intentionally included or inserted in a system for a harmful purpose, commonly referred to as malware. Most common examples are computer viruses and other kinds of spyware (unauthorized programmes) installed to monitor a consumer's activities without consent.

(b). Network Attacks: These are basically actions taken to disrupt, deny, degrade or destroy information residing on a computer and computer networks. It may take the form of fabrication, interception, interruption and modification of information. One hears of terminologies like Denial of Service (Dos) and Distributed Denial of Service (DDos), among others.

(c). Network Abuse: These include fraudulent activities committed with the aid of a computer. SPAM (sending of unsolicited commercial mails from harvested email addresses) is a common example.

(d). Social Engineering: This occurs when people are manipulated into performing actions or divulging confidential information such as through e-mail phishing.

III. EFFECTS OF CYBERCRIME

Since the Internet allows digital anonymity, it is used by persons with ill intentions in ways that negatively affect the population both in the online and offline worlds. Crime such as identity theft is a common example. This occurs especially when one believes a request for personal information is coming from trusted and genuine sources such as banks or other financial institutions, only for the criminal to access the bank and credit accounts or open accounts and destroy the victim's credit rating.

Takeover of businesses by hackers to steal company information or use of company servers for nefarious purposes is another negative example. The high cost of piracy in monetary losses and its negative effects on the entertainment, music and software industries cannot be overemphasized. The effects of a single, successful cyberattack can have far-reaching implications including financial losses, theft of intellectual property, and loss of consumer confidence and trust. The overall monetary impact of cybercrime on society and government is estimated to be billions of shillings per year. In 2012, Deloitte Company noted that banks in East Africa alone lost about Kenya Shillings (Kshs) 4 billion to fraudsters who took advantage of weak security mechanisms[11].

---

[7] See, e.g., Fitzgerald, above n 2,953.
[8] See Barrett, above n 7.
[9] Ibid.
[10] Ibid.
[11] See Lilian Ochieng, 'Tough Law to Boost Fight Against Cybercrime' *Daily Nation Kenya*, 28 January 2014.

IV. STATE OF CYBERCRIME LAW IN KENYA

Kenya has for a long time lacked proper mechanisms to counter cybercrime. A cybercrime countermeasure is defined as an action, process, technology, device or system that serves to prevent or mitigate the effects of a cyberattack against a computer, server, network or associated device. A countermeasure can either be technical or regulatory; technical in the sense that computer and network users are advised to use internet protection such as strong, unique passwords to protect themselves from hackers while regulatory measures include legal frameworks that define and detail the conditions for prosecution of cybercrime.

In Kenya, the Kenya Information and Communications Act of 2009[12] establishes a body known as the National Computer Emergency Response Team (CERTS), whose mandate is to fight cybercrime in Kenya. Kenya has chaired the Cyber Security Taskforce of the East African Regulatory Postal and Telecommunication Organization (EARPTO) whose main objective is to facilitate the establishment of national CERTS in the East African region. In February 2012, Kenya entered into an agreement with a United Nations agency on the implementation of a national focal point for coordinating responses to cybersecurity incidents in the country.

The Kenyan government, through the Communications Authority[13] also signed an Administrative Agreement for the implementation of the Kenya National Computer Incident Response Team Coordination Centre, which would be the national trusted organ for advising and coordinating responses to cybersecurity incidences in Kenya, liaising with the local sector computer incident response teams, gathering and disseminating technical information on computer security incidents, carrying out research and analysis on computer security, thus facilitating the development of key public infrastructure and capacity building in information security.

The Kenyan government is working with the International Criminal Police Organization (INTERPOL) to combat cybercrime in Kenya. Consequently, Kenya is able to leverage on INTERPOL's technical guidance for combating cybercrime, including detection, forensic evidence collection, and investigation. An information technology crime investigation manual provides a technological law enforcement model to improve the efficiency of combating cybercrimes.

Kenya has also made several attempts in its laws to seek to curb cybercrime, the most distinct being the amendment to the Evidence Act[14] to allow the admissibility of digital evidence in court. However, this is not conclusive as the Interpretation and General Provisions Act[15] has not been amended and still requires the production of a physical document for purposes of adducing evidence in court. This means that the production of information and evidence generated, sent or stored in magnetic, optical or computer memory is still contentious. Another law covering this area is the Central Depositories Act[16] which provides stiff penalties for manipulation of electronic data.

V. CHALLENGES

The main challenge with the Kenyan legal regime is that The Kenya Information and Communication Act[17] mostly relates to electronic and mobile transactions and contains only few sections which deal with issues of cybercrime in the country. Moreover, the detailed procedural law provided for in the Convention on Cybercrime[18] is also lacking. One can therefore legitimately argue that this law was not enacted with cybercrime, as we currently know it, in mind. Again as already seen, there is apparent lack of uniformity in the diverse pieces of legislation amended ostensibly to deal with cybercrime. The other challenge relates

---

12 Chapter 411A of the Laws of Kenya.
13 Ibid.
14 Chapter 80 of the Laws of Kenya.
15 Chapter 2 of the Laws of Kenya.
16 Act No 4 of 2000 (Laws of Kenya).
17 Ibid.
18 The *Convention on Cybercrime (The Budapest Convention on Cybercrime)*, opened for signature 23 November 2001, CET 185 (entered into force 1 July 2004).

to investigation and prosecution of cybercrimes. This is evidenced by limited understanding of information and technology issues and cybercrimes and its modus operandi by law enforcement officers who end up applying obsolete investigative techniques for sophisticated cybercrimes. Closely related to this challenge is the issue of processing of digital evidence in which Kenya lacks massively as there is no digital forensic laboratory for such kinds of crimes.

It is with the these realizations that in early 2014, the Office of the Director of Public Prosecution and the Kenya Law Reform Commission began the process of developing the Cyber Crime and Computer Related Crimes Bill, 2014[19] which seeks to equip law enforcement agencies with the necessary legal and forensic tools to tackle cybercrime, which is said to have cost the Kenyan economy nearly Kshs. 2 billion in 2013. The Director of Public Prosecutions has also established a special dedicated unit that will handle all cybercrime related cases in the country.

The draft bill is to address offences against confidentiality, integrity and availability of computer data and systems. This bill, if passed, will go down as the most effective cybersecurity law in Kenya as it makes provision on use of electronic evidence against the accused and at the same time focuses on police investigations and prosecutions. Evidence generated from a computer system will also be admissible in a court of law while prosecuting such a crime. The bill has introduced strict regulations that restrict internet usage and online protection of data such that a person is required to have a digital certificate to transact online. This will enable the authorities to know who is committing which crime online.

The bill gives courts within the country jurisdiction to try any Kenyan citizen who commits an offence anywhere in the world. Those found guilty of committing the offence on a ship or aircraft registered in Kenya, using a Kenyan domain name or outside the territory of Kenya will also be prosecuted in Kenyan courts. They will either be fined Kshs. 2 million, be imprisoned for three years or face both penalties.

The bill also proposes that a person, who causes a computer system to perform its functions, knowing that the access they intend to secure is unauthorized, commits an offence. It also proposes that a person who sells, lets to hire, distributes, publicly exhibits through a computer system, and puts into circulation, or for purposes of sale, hire, distribution, public exhibition or circulation, makes, produces or have in their possession any obscene book, pamphlet, paper, drawing, painting or any obscene object commits an offence.

Those using computers to threaten, abuse or use insulting words or behaviour, display, publish or distribute written or electronic material; or distribute, show or play a recording of visual images will be held accountable. The bill also proposes action against a person who uses a computer system including electronic communication to harass, intimidate or cause substantial emotional distress or anxiety to another person. These include communicating obscene, vulgar, profane, lewd, lascivious, or indecent language, pictures or images. Courts will also issue a warrant authorizing a police officer or lawful authority, to enter any premises to access, search and seize the thing or computer data.

All public or private corporations processing personal data will be expected to report any security breaches resulting in theft, loss or misuse of data to the police, and those who fail to do so will be committing an offence

VI. CONCLUSION

We are of the arguable view that, to date, no legislation has succeeded in totally eliminating crime from the globe and so is the case with cybercrime. Recent experiences show that Kenya's cybersecurity remains quite weak, exposing mobile phone subscribers and internet users to data interception and also making it difficult to prosecute cybercrime suspects. This follows the arrest of 37 Chinese citizens who were arrested in Runda Estate, Nairobi on December 2, 2014. They were allegedly found in possession of laptops, routers and mobile phones and were believed to be preparing to instigate serious crimes. The biggest challenge in prosecuting such crimes is lack of legal framework. Further, in April 2014, a Bangladeshi hacker was able

[19] The Draft Cybercrime and Computer Related Crimes Bill, 2014. For a detailed critique of the bill, see ARTICLE 19, Analysis of the Draft Cybercrime Law of Kenya, 2013 at <www.article19.org/.../Kenya-Cybercrime-Bill-129072014-BB.pdf> 5 May 2015.

to access a Kenyan domain belonging to major service providers such as Google, Microsoft, LinkedIn, HP and Dell. Millions of users on the networks were redirected to the hacker's site which showed the message that the sites had been hacked. This reveals the high level of exposure to cybercrime in the country and worldwide. Needless to say, cybercriminals require close cyber-expert surveillance since the anonymity associated with these crimes makes detection onerous.

Based on the foregoing analysis we propose the enactment of the Cyber Crime and Computer Related Crimes Bill 2014 as it contains comprehensive deterrence measures and a legal framework for prosecution of cybercrimes.