Available online at www.elixirpublishers.com (Elixir International Journal)

International Law

Elixir Inter. Law 116 (2018) 50164-50169

ISSN: 2229-712X

Law Enforcement in the Kenyan Cyberspace: Legal and Forensic Challenges

Jackson Bett
Lecturer, School of Law, University of Nairobi, Kenya.

ARTICLE INFO

Article history:
Received: 17 January 2018;
Received in revised form:
4 March 2018;
Accepted: 16 March 2018;

Keywords
Cybercrime,
Cyberspace,
Data protection,
Obfuscation and
Jurisdictional barriers.

ABSTRACT
The growth of the internet has created numerous opportunities for Kenyans. The last quarter of 2016/2017 financial year, 11.9 million people had access to high-speed internet. Kenya lacks a proper legislative framework to protect the internet consumers from cybercriminals and crypto-anarchists. Kenya is also yet to implement the African Union Convention on Cybercrime and Data protection. The law enforcement agencies in Kenya have struggled to keep up with the policing demands of the digital era. The Kenyan Cybercrime Investigators usually face a steep learning curve because hackers are usually discovering ways to carry out their attacks with little or no detection. The anonymity of the internet spurred by the existence of programs such as the tor browser and tails operating system make it difficult for the law enforcement agencies to enforce the law in Kenya. The lack of a comprehensive legislation on cybercrime creates Nullum crimen disparities that hinder the cross-border investigations of cybercrime. Cybercrime-investigators in Kenya have only been able to successfully prosecute the hybrid cybercrimes that involve traditional offences aided by the use of ICT. Cybercriminals operate with impunity in the Kenyan cyberspace because of the limited expertise and low funding of the Cybercrime Unit in Kenya. The windows OS handicap coupled with jurisdictional barriers, encryption, obfuscation and high evidential threshold in admitting electronic evidence, have led to very low conviction rates of cybercrime offenders in Kenya.

Introduction

Law enforcement on the internet has been a challenge not only to Kenya but the whole world as well. Bruce Sterling (1993) described the internet as a functional and a modern form of anarchy which was beyond government regulation.[1] The anonymity of the internet and the ability to operate pseudonymously from any location of the world has given cybercriminals the leeway to operate with impunity in the cyberspace.[2] As cybercrime incidences that were reported to law enforcement agencies began to increase astronomically, there was a need for international collaboration in curbing the rise of cybercrime.[3]

The Budapest Convention on Cybercrime was the first international legal instrument to attempt to bring civility on the internet where chaos was the order of the day. As governments and regional bodies around the world began enacting legislations to curb the crime in the cyberspace, criminal elements in the cyberspace retreated and regrouped into the dark web.[4] Crypto-anarchists have shown relentless determination to forge an online society without the rule of law where they can operate unfettered. Cybercriminals and crypto-anarchists have created online spaces known as cypher sphere where they operate anonymously rendering copyright laws, content regulation and taxation unenforceable.[5]

Initially, cybercrime offenses were seen as a developed countries problem because developing and less developing countries had low internet penetration, and as such laws and regulations could not be formulated to deal with a problem, they were not facing. According to the Communications Authority of Kenya, internet penetration reached 88% in 2015 with over 37.8 million subscribers accessing the internet. In the first quarter of 2016/2017 financial year, 11.9 million people had access to high-speed internet either through mobile phones or laptops.[6] The high level of internet penetration in Kenya opened up opportunities where

[1]Lewis, BC (2004), 'Prevention of Computer Crime amidst International Anarchy',41 American Criminal Law Review, 1353.
[2] ibid
[3]Linah Benyawa, 'Agency says 3000 cyber-crime cases reported in Kenya monthly' (Standard Media, 7 June 2016) <https://www.standardmedia.co.ke/business/article/2000204352/agency-says-3000-cyber-crime-cases-reported-in-kenya-monthly> accessed 16 February 2017.

[4] Burden, K, Palmer, C and Lyde, B (2003), 'Cyber-Crime: A New Breed of Criminals?', 19(3) Computer Law and Security Report, 222
[5] Clough, J.(2011).Cybercrime.Commonwealth Law Bulletin, 37(4), 671-680.
[6] Communications Authority of Kenya (2016),' First Quarter Sector Statistics Report for The Financial Year 2016/2017(July-September 2016.' CAK. Nairobi, 21-27.

Tele:
E-mail address: jbett@uonbi.ac.ke

cybercriminals can operate easily because the country did not have adequate laws to protect internet consumers in Kenya. Even before the high-speed internet was introduced, Kenyans were facing another unforeseen challenge emanating from mobile money transfer fraud. Through social engineering, fraudsters would trick people into transferring them money, and since the majority of the SIM cards were unregistered, it would be difficult to trace the offender and prosecute them.[7]

The Government of Kenya in the recent past has taken measures to protect the communications and e-commerce infrastructure from cybercrime in the country. Such measures are the registration of SIM cards before they are used, requirements for biometric-identification of customers withdrawing money from the bank and establishing a special division to deal with cybercrime at the CID. However, cybercrimes and crypto-anarchists, have resulted in the use of obfuscation, virtual private networks (VPN), crypto-currencies and tails operating system, to forge a lawless society online beyond the reach of domestic legislation.[8] The National Assembly has given low priority to cybercrime legislation which is needed to eliminate loopholes that exist in the legal framework. Cybercrime offenses have low conviction rate in the courts, and most of the crimes that are detected are hybrid crimes; where traditional crimes were committed with the aid of computers. The borderless nature of cybercrime requires international cooperation and coordination to prosecute the offender.[9] In the subsequent sections, we shall examine the challenges that cybercrime investigators face in prosecuting cybercrime and finally make recommendations on how to protect Kenyans from cybercrimes and crypto-anarchists.

Challenges to law enforcement on the internet

The internet has created a new domain of operations known as the cyberspace. Cybercrime investigators are facing a new class of attacks such as social engineering attacks, vishing, Distributed Denial of Service (DDoS) attacks, cyberespionage and cyber terrorism. The Russian interference into the 2016 US elections demonstrated to the cybercrime investigators around the world the potency of cybercrime in the digital era.[10] Kenya has faced similar problems ranging from DDoS of Kenyan government websites to SIM Card fraud. Several Chinese nationals were arrested in Kenya for operating a cybercommand centre.[11] One of the challenges that face law enforcement in the Kenyan cyberspace is the Windows OS handicap. The majority of the cybercrime investigators are trained with Windows Operating System. Cybercriminals have discovered this OS handicap and resorted to the non-traditional operating systems such as Xenix, Solaris, QNX and Kondara Linux to execute cyber-attacks. Sophisticated cybercriminals usually turn to the Tor Browser in order to mask their location and the Tails Operating system to prevent detection. Hackers and crypto-anarchist usually work hard to discover new exploits and new ways of outmaneuvering law enforcement agencies around the world.[12] Another challenge that is faced by the Cybercrime Unit at the CID in Kenya is that information on how to carry out cyberattacks is readily available for anyone to learn. The trading of hacking tools among the Kenyan hackers and winnable hackers is common and yet there is no comprehensive legislation prohibiting the sale and distribution of hacking tools. Obfuscation and encryption are some of the challenges that cybercrime investigators face when they raid a cybercrime scene.[13] Storage devices are commonly disguised to look like the other household goods. Through stenography, information that would incriminate the offenders is smuggled through media files such as photos, word documents and videos and as such eluding detection by law enforcement agencies.[14] Cybercriminals also use VoIP calls to transmit packages of data through steganograms which are later reconstructed by the recipient to form meaningful data. Cybercrime investigators in Kenya face a steep learning curve because for a successful conviction they must have a higher expertise than the offenders.

It is without a doubt that cybercrime is becoming a national menace and is seen as a threat to our democracy. During the 2017 General Elections in Kenya, the security and the integrity of the Kenya Election Management Information System (KEMIS) was put into question after the murder of Chris Musando who was the ICT chief in IEBC[15]. In March 2017, KRA reported to have lost 4 Billion of its revenue through a series of cyber-attacks. The Serianu Cybersecurity Report on Kenya showed that the financial services sector lost approximately KES 20 billion due to cybercrime in 2016. The cost of cybercrime is equivalent to 0.07% of the country's GDP.[16] Despite the clear menace that is facing the country regarding cybercrime, the majority of the offenders are not identified, and those who are identified have low conviction rates.

Reliance on circumstantial evidence

Prosecution of cybercrime largely relies on circumstantial evidence as the offender must demonstrate that the offender had legal control of the device that was used to commit the crime. The admissibility of electronic evidence is largely governed by section 106B of the Evidence Act. Section 106B outlines the conditions which must be met for electronic documents to be admitted as evidence. The

[7] Leibolt, G. (2010). The Complex World of Corporate Cyber Forensics Investigations. In J. Bayuk (Ed.), CyberForensics (pp. 7-27).

[8] ibid

[9] Johnston, DR and Post, DG (1996), 'Law and Borders – The Rise of Law in Cyberspace', 48 Stanford Law Review, 1367.

[10] Jeremy Diamond, 'Russian hacking and the 2016 election: What you need to know' CNN (16 December 2016) <http://edition.cnn.com/2016/12/12/politics/russian-hack-donald-trump-2016-election/> accessed 16 February 2017.

[11] Ernst, D. (2014). 77 Chinese nationals arrested near U.S. Embassy in Kenya with hacking tools. [online] The Washington Times. Available at: http://www.washingtontimes.com/news/2014/dec/4/77-china-nationals-arrested-us-embassy-kenya/ [Accessed 11 Jul. 2017].

[12] eFevre, K., D.J. DeWitt, & R. Ramakrishnan, 2005, "Incognito: Efficient full-domain k-anonymity", in Proceedings of the 2005 ACM SIGMOD international conference on Management of data, ACM, pp. 49–60.

[13] Don Libes, Obfuscated C and Other Mysteries, John Wiley & Sons, 1993, pp 425.

[14] ibid

[15] Reporter S, "NASA condemns shocking murder of Chris Msando"(The StandardJuly 31,2017) <https://www.standardmedia.co.ke/article/2001249871/nasa-condemns-shocking-murder-of-chris-msando> accessed August 4, 2017

[16] "Cyber crimes may cost Kenya 'Sh20bn' in 2017" (The Star, KenyaMay 30, 2017)<http://www.the-star.co.ke/news/2017/05/31/cyber-crimes-may-cost-kenya-sh20bn-in-2017_c1570688> accessed August 4, 2017

prosecution must demonstrate that the document was produced when the person producing the document had lawful control of the device producing the document. It is easy to challenge the admissibility of evidence under this section because hackers can still have control over the device long after the crime was committed and might tamper with the production of the documentary evidence. The second condition that must be met is the information that is fed into the computer or the kind of information from which such record is derived was regularly fed into the computer in the ordinary course of business. The third condition requires the prosecution to demonstrate that the computer was working properly when the evidence was produced. In the event that there are software errors, the evidence would be inadmissible. It is not clear what the parliament meant by working properly. Computer systems are usually subject to several failures some of which affect the performance of the computers and other failures just make some functions to be inaccessible. The language of the legislation is a hindrance to the prosecution of hackers and crypto-anarchists. The fourth condition is that the information was fed in the ordinary course of business. It is difficult to demonstrate to the court that during the investigation, the computer was free from any remote interference.

The challenges relating to the admissibility of electronic evidence were seen in Republic v Mark Lloyd Steveson [2016] eKLR, where an email which was instrumental to the case was determined to be inadmissible for failure to adhere to the rules of admission under the Evidence Act. The prayer was dismissed on the basis of lack of proper authentication in admitting evidence.

The computer-generated evidence is usually considered hearsay evidence without a certificate of authenticity. Section 106 (B) states that electronic evidence must be accompanied by a certificate. The person who generated the electronic evidence must also swear upon its accuracy and authenticity. Before the police can commence investigations, they require a search warrant except under the plain view doctrine and in the case of national emergency. The actual investigation can be complex as it entails going through terabytes of data just from one household. Collecting data from confiscated devices has also been a challenge for cybercrime investigators because modern devices come with pre-installed data sanitation tools that enable the user to wipe all the data remotely.[17] They also have pre-installed anti-forensic tools to protect the user from intrusion. In the Apple-FBI Encryption dispute, FBI were unable to access the data stored on an iPhone that was crucial for a terrorism investigation. FBI had to procure the services of a professional hacking team in order to access the data.[18] Investigators in Kenya face similar problems, but with limited resources and lack of expertise, they are unable to decipher the data contained in the phones.

Cloud computing has become another investigative hurdle that cybercrime investigators encounter. Data stored in the cloud can be accessed from any location in the world. Cloud computing services are considered to be innately global and beyond the scope of most of the domestic laws.[19] Cloud computing has given child pornography traffickers an avenue to distribute prohibited material without being caught. The users can access the data from the cloud using login details. Once detected the crime usually spans through multiple jurisdictions making it difficult to prosecute.[20]

Jurisdictional barriers

The infrastructure of the internet makes it possible for a crime to be committed in a different country when the offender is located in another country. Cybercrime has repeatedly caused damage worldwide with the computer systems that support the critical infrastructure becoming subject to global malware intrusion. A global cyber-attack has the potential of causing $ 121.4 billion loss which is equivalent to the damage caused by Hurricane Katrina.[21] The global attacks such as WannaCry[22] hackers raised the need for international cooperation in combating cybercrime. In order to effectively thwart cyber-attacks, there is a need for global cooperation which will entail governments and private corporations.

Jurisdiction defines the legal authority of a sovereign country to pursue investigations. Kenyan cybercrime investigators have come to see court as the invisible barrier that prevents the prosecution of crime across borders.[23] There are two types of jurisdiction; the first one is subject matter jurisdiction and the other one is personal jurisdiction. Personal jurisdiction refers to whether the court has power over the persons of interest.[24] In Kenya, the cybercrime prosecutors must examine the personal and subject-matter jurisdiction in order to determine whether the matter will have any legal standing before the court. International and regional bodies have come together to form a legal framework for the prosecution of cybercrime because if the jurisdictional problem is not handled the number of cybercrime victims will continue to increase.[25] The council of Europe came together to formulate the Budapest Convention on Cybercrime. The African Union came with the African Union Convention on Cybercrime and Personal Data protection. The AU convention on cybercrime gives protection on the internet users on e-commerce fraud and requires member states to foster the growth of e-commerce in

[17]Zeigler AD and Rojas EF, Preserving electronic evidence for trial: a team approach to the litigation hold, data collection, and evidence preservation (Elsevier 2016)

[18]Lichtblau KBE, "U.S. Says It Has Unlocked iPhone Without Apple" (The New York TimesMarch 28, 2016) <https://www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html?_r=0>accessed August 4, 2017

[19]Alexander Seger, 'Evidence in the cloud and the rule of law in cyberspace -Europe's world' (Security Europe, 7 December 2015) <http://europesworld.org/2015/12/07 /evidence-cloud-rule-law-cyberspace/#.WKX2Z_l9600> accessed 16 February 2017.

[20] ibid

[21]Suess O, "Global Cyber Attack Could Cost $121.4 Billion, Lloyd's Estimates"(Bloomberg.com July 18, 2017) <https:// www.bloomberg.com/news/articles/2017-07-18/global-cyber-attack-could-cost-121-4-billion-lloyd-s-estimates> accessed August 4, 2017

[22]WannaCry is the name used to refer to the global ransomware attack that took place in May 2017. The ransomware targeted Windows Operating Systems and required its victims to pay in order to gain access to their documents.

[23]Teng, A. (2017).Jurisdictional Barriers: Cybercrime Prosecution Challenges (Doctoral dissertation,Utica College).

[24] ibid

[25]Kirby,M. D.(2008).The Urgent Need for Forensic Excellence.Criminal Law Journal, 32.

their respective countries. Kenya should ratify and implement these regional and international Conventions to deal with the challenge of prosecuting cybercrimes.

Dual criminality

For international co-operation to be achieved, there needs to be dual criminality between the two countries. Lack of global cooperation has weakened the principle of dual criminality. The dual criminality means that the offense committed must be recognized as a criminal offense for the individual to be extradited to face prosecution in another country.[26] For instance, the offenders who were behind the Love Bug virus in 2000 were able to escape prosecution because the offense they committed was not recognized as a crime under the Philippines law.[27]

The principle of Nullum crimen sine lege states that an act is not considered to be a crime without law.[28] Kenya lacks a comprehensive legislation which criminalizes offenses such as packet sniffing and trade of hacking tools. The possession of a hacking software or carrying out Distributed Denial of Service Attacks is considered to be immoral but not illegal. The Nullum Crimen disparities have made it difficult to successfully prosecute cybercrimes in Kenya. Russia, for instance has passed laws aimed at asserting its network sovereignty. Cybercrime investigators are considered to be violating Russian sovereignty while probing servers located in Russia for the evidence to prove that a crime was committed.[29] The lack of cooperation between nations in prosecuting cybercrime has been exploited by cybercriminals.[30] The tor browser and Tails operating system enable hackers to mask their actual location and eliminate all the evidence of their crime. Nullum Crimen Disparities have forced Kenyan cybercrime investigators to focus largely on domestic offenses.

Under Reporting

Most of the cybercrimes in Kenya usually go unreported. Civilians have low confidence in the ability of the police to investigate and bring the offender to justice. The majority of cybercrimes that have caught the attention of the police are credit card fraud, M-pesa Fraud and identity theft. In identity theft, the offender takes the persona of the victim and might incur liabilities which are borne by the victim.Cybercriminals usually steal personal details and sell them in the black market.[31] This blatant violation of privacy most of the time goes unnoticed because the victims never notice that their personal details have been stolen. Financial institutions in Kenya have borne the brunt of cybercrime with a total loss of KES 17.7 billion. Financial institutions do not usually go public with information about hacking because of the fear of negative publicity. It is suspected the amount is higher because the banks want to maintain a positive image before the public.

Recommendations and Conclusion

Cybercrime is one of the greatest challenges to social order in the modern world. The internet has brought up numerous opportunities and created a new class of crimes as well. The internet is crucial for the prosperity and well-being of the people of Kenya. Initially, the internet started as an anarchist online society that was largely unregulated and out of the reach of domestic legislation. The problem was further exacerbated by the ability for cybercriminals and crypto anarchists to browse the internet anonymously.[32] The existence of tools such as tor browser and Tails operating system have enabled cybercriminals and crypto-anarchists to operate with impunity. Governments around the world began making inroads in the otherwise unregulated sphere to protect their citizen from cybercrime.[33]

One of the greatest barriers that regulators face regarding cybercrime is the jurisdictional barrier. Kenya should collaborate with other countries to ensure that offenders do not use the Kenyan cyberspace as their playing ground. Currently, Kenya does not have a comprehensive legislation

on cybercrime and data protection. The National Assembly should pass the Computers and Cybercrime Bill that is still pending in parliament. This bill will establish a Cybercrime Unit that will be responsible for safeguarding the Kenyan cyberspace from cyberattacks. The bill if passed will eliminate the Nullum crimen disparities that have hindered the cooperation of Kenya with other countries in prosecuting cybercrime. The current legal framework on cybersecurity is comprised of Kenya Information and Communications Act (Amendment) (Cap 411), Evidence Act (Cap 80), The Penal Code (Cap 63), The Proceeds of Crime and Anti-Money Laundering Act, No.9 of 2009, The Criminal Procedure Law (Cap 75), The Sexual Offences Act (2006) and Central Depositories Act 2017. In addition to passing the Computers and Cybercrime Bill, the National Assembly should also pass the Critical Infrastructure Bill 2016 and Data Protection Bill 2013.

Kenya should implement the African Union Convention on Cybercrime and Data Protection. The overarching legislation by the African Union seeks to tackle three areas that are not protected in the cyberspace. These sections are; electronic transactions, personal data protection and cybercrime. By focusing on those areas, the African Union hopes to foster development and secure the cyberspace from criminals. Article 25 of the convention requires national governments to come up with cybersecurity policy and assign responsibilities of protecting the critical infrastructure from cybercriminals. Kenya should implement the African Union Convention on cybercrime and Data Protection. Kenya should also join the Budapest Convention on Cybercrime. Although the convention was primarily made for European Union

[26] Hudson, Manley O. "The Factor Case and Double Criminality in Extradition." The American Journal of International Law 28.2 (1934): 274-306.

[27] Rasch M, "Cybercrime treaty flawed, but needed" (Cybercrime treaty flawed, but needed2001) <http://www.securityfocus.com/columnists/11> accessed August 4, 2017

[28] Aly Mokhtar; Nullum Crimen, Nulla Poena Sine Lege: Aspects and Prospects, Statute Law Review, Volume 26, Issue 1,1 January 2005,Pages 41–55, https://doi.org/10.1093/slr/hmi005

[29] Georgios I. Zekos, Dr.; State Cyberspace Jurisdiction and Personal Cyberspace Jurisdiction, International Journal of Law and Information Technology, Volume 15, Issue 1, 1 March 2007, Pages 1–37, https://doi.org/10.1093/ijlit/eai029

[30] ibid

[31] Scott Charney, Rethinking the Cyber Threat: A Framework and Path Forward, Trustworthy Computing Group, Microsoft Corporation, 2009, p. 12.

[32] Nuth, M. S. (2008). Crime and technology – Challenges or solutions? Taking advantage of new technologies: For and against crime.Computer Law & Security Report, 24, 437–446.

[33] Maryann Cusimano Love. (2011). Beyond Sovereignty: Issues for a Global Agenda. Wadsworth, Cengage Learning.

countries, other countries have ratified the treaty. For instance, Mauritius and South Africa are parties to the treaty.[34] It is important to recognize that Russia refused to ascend to the treaty citing that it violated its network sovereignty. The Budapest convention encourages sharing of electronic evidence between countries with the objective of countering the spread of cybercrime.[35]

There is an urgent need to training members of the judiciary and cybercrime investigators on the cybercrime. The majority of the magistrates and judges serving in our judiciary joined the bar when the cyberlaw discipline was at its infancy at the international level. Since then, Cyberlaw has evolved to become a very reputable discipline of law. The proper interpretation of cybercrime and data protection laws is crucial in ensuring that cybercriminals are convicted of their crimes. The members of the bench should be trained on a regular basis on how to handle cyberlaw issues that are brought before them[36]. In order to prepare the future generation of lawyers and members of the bench on handling cybercrime issues, cyberlaw should be introduced as a unit in law schools across the country and also in the Kenya School of law. Cybercrime investigators in Kenya usually face the Windows OS handicap. They should be trained on a regular basis on the use of other operating systems that have become very common with the cybercriminals.

In conclusion, cybercrime has become a national security issue in Kenya. With 11.9 million people having access to high-speed internet, there is a need to protect the Kenyan internet consumers. The infrastructure of the internet has created zones that are out of the scope of the law. Governments have made a lot of inroads in regulating the indexed part of the internet. The National Assembly should pass the relevant laws to ensure that the users of the Kenyan cyberspace are protected from cybercriminals and crypto-anarchists.

Bibliography

Cases and Legislation

Cases

Republic v Mark Lloyd Steveson [2016] eKLR

Legislations

1. Kenya Information and Communications Act (Amendment) (Cap 411)
2. Evidence Act (Cap 80)
3. The Penal Code (Cap 63)
4. The Proceeds from Crime and Anti-Money Laundering Act, No.9 of 2009
5. The criminal Procedure Law (Cap 75)
6. The Sexual Offences Act (2006)
7. Central Depositories Act 2017

Conventions

1. Convention on Cybercrime of the Council of Europe (CETS No.185)
2. African Union Convention on Cyber Security and Personal Data Protection

[34]Vatis, Michael A. "The Council of Europe Convention on Cybercrime." Proceedings of the Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options. 2010.

[35] Convention on Cybercrime, Budapest, 23 November 2001.

[36]Council of Europe, "Cybercrime training for Judges and prosecutors: a concept" [2009] Department of Information Society and Action against Crime Directorate General of Human Rights and Legal Affairs Strasbourg, France

Books

1. Maryann Cusimano Love. (2011). Beyond Sovereignty: Issues for a Global Agenda. Wadsworth, Cengage Learning.
2. Don Libes, Obfuscated C and Other Mysteries, John Wiley & Sons, 1993, pp 425.

Journal Articles

1. Aly Mokhtar; Nullum Crimen, Nulla Poena Sine Lege: Aspects and Prospects, Statute Law Review, Volume 26, Issue 1, 1 January 2005, Pages 41–55, https://doi.org /10.1093/slr/hmi005.
2. Burden, K, Palmer, C and Lyde, B (2003), 'Cyber-Crime: A New Breed of Criminals?', 19(3) Computer Law and Security Report, 222.
3. Clough, J. (2011). Cybercrime. Commonwealth Law Bulletin, 37(4), 671-680.
4. Georgios I. Zekos, Dr.; State Cyberspace Jurisdiction and Personal Cyberspace Jurisdiction, International Journal of Law and Information Technology, Volume 15, Issue 1, 1 March 2007, Pages 1–37, https://doi.org/10.1093/ijlit/eai029.
5. Hudson, Manley O. "The Factor Case and Double Criminality in Extradition." The American Journal of International Law 28.2 (1934): 274-306.
6. Johnston, DR and Post, DG (1996), 'Law and Borders – The Rise of Law in Cyberspace', 48 Stanford Law Review, 1367.
7. Kirby, M. D. (2008).The Urgent Need for Forensic Excellence. Criminal Law Journal, 32.
8. Leibolt, G. (2010).The Complex World of Corporate Cyber Forensics Investigations. In J. Bayuk (Ed.), CyberForensics (pp. 7-27).
9. Lewis, BC (2004), 'Prevention of Computer Crime amidst International Anarchy', 41 American Criminal Law Review, 1353.
10. Nuth, M. S. (2008). Crime and technology – Challenges or solutions? Taking advantage of new technologies: For and against crime. Computer Law & Security Report, 24, 437–446.

Reports

1. Communications Authority of Kenya (2016),' First Quarter Sector Statistics Report for the Financial Year 2016/2017(July-September 2016.' CAK. Nairobi, 21-27.
2. Council of Europe, "Cybercrime training for Judges and prosecutors: a concept" [2009] Department of Information Society and Action against Crime Directorate General of Human Rights and Legal Affairs Strasbourg, France.
3. LeFevre, K., D.J. DeWitt, & R. Ramakrishnan, 2005, "Incognito: Efficient full-domain k-anonymity", in Proceedings of the 2005 ACM SIGMOD international conference on Management of data, ACM, pp. 49–60.
4. Scott Charney, Rethinking the Cyber Threat: A Framework and Path Forward, Trustworthy Computing Group, Microsoft Corporation, 2009.
5. Teng, A. (2017). Jurisdictional Barriers: Cybercrime Prosecution Challenges (Doctoral dissertation, Utica College).
6. Vatis, Michael A. "The Council of Europe Convention on Cybercrime."Proceedings of the Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options. 2010.

Periodicals

1. "Cybercrimes may cost Kenya 'Sh20bn' in 2017" (The Star, KenyaMay 30, 2017) <http://www.the-star.co.ke/news/2017 /05/31/cyber-crimes-may-cost-kenya-sh20bn-in-2017_c1570688> accessed August 4, 2017.

2. Alexander Seger, 'Evidence in the cloud and the rule of law in cyberspace - Europe's world' (Security Europe, 7 December 2015) <http://europesworld.org/2015/12/07/evidence-cloud-rule-law-cyberspace/#.WKX2Z_l9600> accessed 16 September, 2017.
3. Ernst, D. (2014). 77 Chinese nationals arrested near U.S. Embassy in Kenya with hacking tools. [online]The Washington Times. Available at: http://www.washingtontimes.com/news/2014/dec/4/77-china-nationals-arrested-us-embassy-kenya/ [Accessed 11 October, 2017].
4. Jeremy Diamond, 'Russian hacking and the 2016 election: What you need to know' CNN (16 December 2016) <http://edition.cnn.com/2016/12/12/politics/russian-hack-donald-trump-2016-election/> accessed 16 October, 2017.
5. Lichtblau KBE, "U.S. Says It Has Unlocked iPhone Without Apple" (The New York Times March 28, 2016) <https://www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html?_r=0>accessed August 4, 2017.
6. Linah Benyawa, 'Agency says 3000 cyber-crime cases reported in Kenya monthly' (Standard Media, 7 June 2016) <https://www.standardmedia.co.ke/business/article/2000204352/agency-says-3000-cyber-crime-cases-reported-in-kenya-monthly> accessed 16 October, 2017.
7. Rasch M, "Cybercrime treaty flawed, but needed" (Cybercrime treaty flawed, but needed2001) <http://www.securityfocus.com/columnists/11> accessed August 4, 2017.
8. Reporter S, "NASA condemns shocking murder of Chris Msando" (The Standard July 31, 2017) <https://www.standardmedia.co.ke/article/2001249871/nasa-condemns-shocking-murder-of-chris-msando> accessed August 4, 2017.
9. Suess O, "Global Cyber Attack Could Cost $121.4 Billion, Lloyd's Estimates"(Bloomberg.comJuly 18, 2017) <https://www.bloomberg.com/news/articles/2017-07-18/global-cyber-attack-could-cost-121-4-billion-lloyd-s-estimates> accessed August 4, 2017.
10. Zeigler AD and Rojas EF, Preserving electronic evidence for trial: a team approach to the litigation hold, data collection, and evidence preservation (Elsevier 2016).