library@chuka.ac.ke; www.chuka.ac.ke

CYBERSECURITY LAWS AND DIGITAL TRANSFORMATION: A SURVEY OF THE STATE-OF-THE-ART

Mohamed H. Abdi
P.O. Box 231-00610 Nairobi. mhabdi@gmail.com Telephone 0722977728
School of Computing and Information Technology, Jomo Kenyatta University of Agriculture and Technology, P. O. Box 62000-Nairobi, Kenya

Citation: Mohamed, H. Abdi. (2016). Cybersecurity laws and digital transformation: A survey of the state-of-the-art. In: Isutsa, D.K. and Githae, E.W. *Proceedings of the Second Chuka University International Research Conference held in Chuka University, Chuka, Kenya from 28th to 30th October, 2015. 325-332 pp.*

ABSTRACT
The objective of this paper is to review the existing literature on Cybersecurity Laws and highlight the major challenges in development and application of the necessary instruments of legislation and how this is impacting on digital transformation and development. The global nature of cybercrime has necessitated an urgent drive towards the enactment and harmonization of Cybersecurity laws if digital transformation and development is to be realized. While that is a noble idea, the sluggish pace at which the legislations are being enacted may render them outdated or inapplicable to the current threats that are abound in the security landscape. This has far reaching implications and consequences to digital transformation and development. The paper is based on a literature review of existing published research on cybersecurity, cybercrime, cybersecurity laws and digital transformation. A survey of existing literature was conducted whose findings are presented. The review has shown that cybercrime is a global problem without geographical borders while enacted legislations are not keeping pace with the changing technology landscape and are not harmonized. Cybercrime statistics are inaccurate as many cases go undetected or unreported. It is costly to develop and maintain security and other preventive measures. While efforts have been made towards digitization and development, African continent lacks the human resource capacity and the technology infrastructure necessary to detect, prosecute and convict the perpetrators of cybercrimes. The study findings are intended to assist business managers to effectively understand Cybersecurity and cybercrime in order to review the related Laws, policies and procedures in tandem with national and international standards and conventions. Digital transformation is first and foremost a business transformation; it is not just about technology. Cybersecurity legislation is an essential ingredient to digital transformation. Africa and indeed the world has to heavily invest in Cybersecurity awareness and skills

development training, conduct focused research in cyber threat, and develop common cybersecurity frameworks.

Keywords: Cybersecurity, Cybercrime, Laws, digital transformation, development, harmonization

INTRODUCTION

Managing digital transformation can be challenging, but awareness of, and preparedness for, analysis of both the resources/capability and external demands through the resource fit perspective are necessary (Liu et al., 2013). Every day new digital applications and equipment find their way into our lives and has permuted every sphere of our life (Marcum, 2014). Information and Communication Technology (ICT) has brought our society many benefits and will continue to do so for the coming years as key driver of change and enabler of economic growth. It is evident that 'Digitization' can extend the reach of organizations, improve management decisions, and speed up the development of new products and services. Furthermore, it can lead to new business opportunities as well as, clearing the path for the competitive edge. According to (Berman, 2014), paths to strategic transformation from research and industry experience can be summarized by three basic approaches: focusing on customer value propositions, Transforming the operating model and combining this two approaches by simultaneously transforming the customer value proposition and organizing operations for delivery. The Government of Kenya cybersecurity strategy has adequately addressed the need for the enactment of cybersecurity laws under goal number three (3) of fostering information sharing and collaboration (*Government of Kenya Cybersecurity Strategy*, 2014).

There are drawbacks to everything, and that includes digitization. As our dependence and reliance on ICT grows, so does our vulnerability. This requires leadership, safeguards and action to mitigate the risks. The African continent is poised to become the new cybercrime haven due to availability of fast Internet access, expanding Internet user base and the lack of cybercrime laws. The growth and adoption of ICT infrastructure and services is not matched by the prerequisite human resource development. Africa lacks both the legislative framework as well as the ability to detect, prevent and bring the culprits to book. However, the growing, sophisticated threats posed by cyber attackers especially as it relates to critical infrastructure, information and services, is not news any more. Recently, it was reported in the mainstream daily newspapers in Kenya of a cyber-attack which targeted and defaced 103 Government of Kenya websites. The hacker, who claims to be part of an Indonesian online forum known us the Forum Code Security, left a message that he will carry out more attacks on servers if the government continues to neglect security.

In other parts of the World, the headlines were not any different; conveying a frightening story of technology-enabled criminal activity. *Conficker Virus Begins to Attack PCs … Canadian Research Uncovers Cyber Espionage Network … Brazil Arrests 10 on Kiddie- Porn Charges … Cyberbullying Affects Half of U.S. Teens* (Neufeld, 2012). Unfortunately, such reports are not the product of mere news writer hyperbole.

The Cyberspace Crime has always been an important but thorny issue in the international community. There are three different aspects of Cyberspace Crime that needs to be addressed across the globe: legislation, law enforcement and technology research (Cheng, 2011). The lack of proper legal and policy frameworks, cybersecurity research, awareness training and regulation and the necessary expertise is hindering the fight against cybercrime(Kritzinger et al., 2013).

The Internet is one of the fastest-growing areas of technical infrastructure development in an unprecedented manner. Africa's current cable infrastructure covers almost the whole of the continent, connecting its citizens with the rest of the world. This was achieved through joint venture bringing together African governments and private companies from different countries worldwide to fund and implement six projects namely SEACOM, EASSy, the East African Marines System (TEAMS), West Africa Cable System, Main One and WASACE to improve Africa's ICT infrastructure (Kharouni, 2013).

Section 2 deals with the methodology used to conduct the literature review. Section 3 will provide a review of the existing literature and also delve into international efforts towards cybercrime legislation. Section 4 will address the challenges. The rest of the paper will look at anti cybercrime strategies, results and conclusions.

METHODOLOGY

It is crucial to conduct a literature review before proceeding with any research study (Hart, 1998). Webster and Watson (2002) emphasize that review of prior relevant research is essential for any academic project and "it facilitates theory development, closes areas where a plethora of research exists, and uncovers areas where research is needed". An effective literature review should involve the leading literature as it is likely to cover the major contributions (Webster et al., 2002). Accordingly, we searched in all Quality Information Systems Literature stated in (Levy and Ellis, 2006) that were accessible from our academic environment and also from our digital library available through professional membership to ACM and IEEE computer Society. In order not to miss any relevant documents, we preferred to perform a broad research and eliminate the irrelevant documents manually. We used the keywords of "digitization", "Cybersecurity legislation" and "Cybercrimes". Each time, we repeated the search also with the keyword "Cyber" to cover different writing styles and areas of interest. After removing the duplicates and irrelevant literature to the area of cybersecurity legislation, we embarked on analyzing the remaining materials under the headings outlined in the following literature review. The Identification of relevant literature involved search through the following electronic resources: The ACM Digital Library, IEEE Computer Society, JKUAT Resources and Google Scholar. The search was implemented on all sources that were accessible through these electronic databases: journals, conference proceedings, books, reference works, online reports and magazine articles.

Defining Digital transformation, Cybersecurity and Cybercrime

Digital transformation refers to the changes associated with the application of digital technology in all aspects of human society. Digital transformation may be thought of as the third stage of embracing digital technologies: digital competence, digital literacy to digital transformation (Lankshear et al., 2008). Digital transformation affects both the individual and the business, private or public. Cybersecurity is a term used to describe the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. Crime may be broadly defined as "any identifiable behavior that an appreciable number of governments has specifically prohibited and formally punished". Cybersecurity is measures relating to the confidentiality, availability and integrity of information that is processed, stored and communicated by electronic or similar means (Nambiro, A. W., Muchiri, 2014). In the context of this paper, Cybersecurity is to be understood as the collection of policies, security safeguards, security concepts, risk management approaches, guidelines, technologies, actions and training that can be used to protect the organization and cyber environment together with the user's assets.

Ensuring Cybersecurity requires coordinated efforts throughout an information system. Elements of Cybersecurity include application security, Information security, Network security, Disaster recovery/business continuity planning and end user education and awareness training (Popa, 2010). Decreasing fear of cybercrime can only be achieved by educating users of the cyberspace (Mesko et al., 2011). Cybercrime is criminal activity done using computers and the Internet, a computer system or computer technology. This includes but not limited to identity theft, illegal downloading and/or circulation of copyrighted materials and fraud among others. It also includes non-monetary offences such as creating and distributing viruses on other computers or posting or stealing confidential business or private information/data (Nambiro, A. W., Muchiri, 2014).

The following is a general (non-comprehensive) list of criminal activity that may fit into this category: Production, distribution and downloading of child abuse material , copyright infringement, software piracy,

trademark violations , online harassment, Distributed denial of service attacks , hacking, advance-fee fraud conducted over the internet, Identity theft and identity fraud, Scams and online frauds, Phishing, Malicious software and spam, Attacks against critical infrastructures and Virtual world or gaming incidents (McCombie et al., 2010). Cases of Cybercrime, prosecution and conviction are rare. However, the sentencing in an Italian criminal court against three top managers of Google received much attention in Italy and abroad. It may be considered a "leading case" on the debate over the criminal responsibility of Service Providers (Marra, 2010). The debate has gone on for some time on where the responsibility of the service provider starts and ends.

Cybersecurity Laws

As computers and computer systems developed, so have also criminal offences associated with their use. The human race will always have to live with criminal activity and as a result of the increased demand and reliance on use of computers and networks by the information society, new methods of perpetrating crimes have been developed and flourished. Traditional penal laws were not written with this new development in mind. The main challenge of applicability of this legislation on cybercrime became evident by the day. In order to establish criminal offences for the protection of information and communication, provisions must be enacted with as much clarity and specificity as possible, and not rely on vague interpretations in the existing laws. When cybercrime laws are adopted, perpetrators will be convicted for their explicit acts and not by existing provisions stretched in the interpretations, or by provisions enacted for other purposes covering only incidental or peripheral acts. One of the most important purposes in criminal legislation is the prevention of criminal offenses (Oluwafemi et al., 2013).

One of the most important purposes in criminal legislation is the prevention of criminal offenses. A potential perpetrator must be given a clear warning with adequate foreseeability that certain offences are not tolerated. And when criminal offences occur, perpetrators must be convicted for the crime explicitly done, satisfactorily efficient in order to deter him or her, and others from such crime. These basic principles are also valid for cybercrimes (Cassim, 2010). When creating cyber laws, developing nations must know that they will be crossing local and international jurisdictional boundaries (Phillips, 2011).

The Pioneers in Cybercrime Legislation

Several individuals were engaged in the fight against computer crime from the early development. The founder and father of the knowledge of computer crime is by many observers considered to be Donn B. Parker, USA. Other authors who have immensely contributed to the fight against computer crime include Bequai and Jay Bloombecker (USA), Stein Schjolberg (Norway), Ulrich Sieber (Germany), H.W.K. Kaspersen (The Netherlands) and K. E. Brown (Australia) (Schjolberg, 2008).

International initiatives in cybercrime legislation

Political or geographical boundaries are not an obstacle to conducting cybercrime, hence global agreements and initiatives are essential to ensure efficient international co-operation. The following is an array of international and multi-lateral initiatives targeting cybersecurity and cybercrimes.

The Council of Europe (COE)

The Council of Europe (COE) established the Budapest Convention of Cybercrime recognized today as an important international instrument in the fight against cybercrime. The main capacity building project and driver of the COE's action against cybercrime has been the Global Project on Cybercrime (Craig Rosewarne, 2012). The Convention on Cybercrime distinguishes between four different types of offences: Offences against the confidentiality, integrity and availability of computer information/systems; computer-related offences, content-related offences and copyright-related offences.

The Budapest Convention on Cybercrime

The Budapest Convention on Cybercrime was one of the first international community efforts to establish a universal treaty on cybercrime. It is the first international treaty seeking to address computer and internet crimes by harmonizing national laws, improving investigative techniques and increasing cooperation among nations. It was opened for signature in Budapest, on 23 November 2001 and it entered into force on 1 July 2004 (Wamala, 2012). The objectives of the Budapest Convention include; Stronger and more harmonized cybercrime legislation worldwide, consistent approach to criminalizing conduct, procedural powers for law enforcement and international cooperation, more efficient international cooperation, more investigation, prosecution and adjudication of cybercrime and a contribution to human rights and the rule of law in cyberspace.

Under the convention, member states are obliged to criminalize; illegal access to a computer system, interception of information to a computer system, interfering with computer system without right, intentional interference with computer information without right, the use of inauthentic information with intent to put it across as authentic (information forgery), infringement of copyright related rights online, interference with information or functioning of computer system and Child pornography related offences (Sarantinos et al., 2013).

African Union Convention on Cybersecurity and Personal Data Protection

African Union Convention on Cybercrime (AUCC) seeks to intensify the fight against cybercrime across African continent in light of the increase in cybercrime, and the lack of mastery of security risks by African countries. Further, a major challenge for African countries is the lack of adequate technological security to prevent and effectively control technological and informational risks. As such, African States are in dire need of innovative criminal policy strategies that embody States, societal and technical responses to create a credible legal climate for Cybersecurity (Grace Githaiga, 2013).

The Convention establishes a framework for Cybersecurity in Africa through organization of electronic transactions, protection of personal data, promotion of cyber security, e-governance and combating cybercrime (Judge et al., 2014). The Convention is intended to:

(a) Define the objectives and broad orientations for the information society in Africa.
(b) Strengthen existing legislations in member states and the regional economic communities on Information and Communication Technologies.
(c) Define the security rules essential to establishing a credible digital space in response to the major security related obstacles to the development of digital transactions in Africa.
(d) Lay the foundation for cyber ethics and fundamental principles in the key areas of Cybersecurity across Africa.
(e) Define the basis for electronic commerce, puts in place a mechanism for combating intrusions into private life likely to be generated by the gathering, processing, transmission, storage and use of personal information and sets broad guidelines for incrimination and repression of cybercrime.

Multi-Lateral cybercrime initiatives

A number of international organizations work constantly to promote or use collective defenses to analyze the latest developments in cyber threats and cybercrime. Some examples include the the United Nations (UN), Commonwealth Internet Governance Forum (CIGF), Forum for Incident Response and Security Teams (FIRST), IMPACT (International Multilateral Partnership Against Cyber Threats), and the International Telecommunication Union (ITU) among others.

The International Cybercrime Assistance Program (ICAP) has been established as one of the programs of work put in place by the International Cybersecurity Protection Alliance (ICSPA) to provide financial support and other forms of practical assistance to law enforcement units engaged in combating cybercrime in those countries that would benefit most from such assistance and who are willing to accept it (ICSPA, n.d.). ICAP seeks to identify countries being used as cybercrime bases and also identify multi-national

companies that are target of such crimes. It also aims to enlist membership, raise funds and provide technical assistance to the willing countries and companies in case of cybercrime investigation.

Challenges of fighting cybercrime

The major challenge to governing cybercrime is the nature of the complex multidimensional virtual world, which does not have any defined physical territorial boundary. The traditional criminal law, which took many years to evolve, does not apply. It is also difficult to obtain accurate cybercrime statistics because an unknown number of crimes go undetected and unreported. It is also costly to develop and maintain security and other preventative measures. It is thus a continuous uphill battle to develop cybercrime legislation that applies to both domestic and international audiences. Cybercrime is threating both the national and international security (Tabansky, 2012).

Other challenges noted by (Bargh et al., 2012) are attributed to democracy and governance. A war against cybercrime in a democratic society is impossible unless there are clear definitions of such crimes and appropriate laws and governance mechanisms to safeguard the rights of all parties. There are numerous challenges faced by law enforcement agencies. Chief among them is the harmonization of national criminal laws regarding to cybercrimes or the difficulties to find an acceptable definition of computer related crime (Jang et al., 2013). If there is no common understanding of the problem, countries do not know how to respond. For instance, it is difficult to find an agreement on common concepts of cybercrime, computer crime or high-tech crimes. Other difficulties include that of locating and identifying perpetrators across borders and Conflicts of jurisdiction. Law enforcement typically stops at the borders of nation states and must go through proper legal channels and procedures to receive assistance in pursuing cybercrime investigations and prosecutions. It also becomes necessary to seek the assistance and support of agencies such as Interpol, Europol, etc. to not only help in the investigations and prosecution processes but also in extradition of criminals from one jurisdiction to another (Cerezo et al., 2007).

Anti-cybercrime strategies

The Global Cybersecurity Agenda (GCA)is designed for cooperation and efficiency, encouraging collaboration with and between all relevant partners and building on existing initiatives to avoid duplicating efforts (Sánchez, n.d.). The GCA has seven main strategic goals, built on five work areas Legal measures, Technical and procedural measures, Organizational structures, Capacity building and International cooperation (Wamala, 2012). African countries should also develop robust Computer Emergency Readiness Teams (CERTs) and Computer Security Incident Response Team (CSIRT) to respond to cyber incidents, provide technical assistance to hacked businesses and disseminate timely notifications regarding current and potential threats. Anti-Cybersecurity regulation proponents argue that laws will inhibit innovation, it is costly and infringes on privacy. Critics of cyberspace regulation are of the view that that the legislation could lead to the curtailment of internet and media freedom.

RESULTS

The literature review study has shown that;

a) Computer systems can be accessed from anywhere in the world
b) Cybercrime is global in nature
c) Traditional boundaries do not apply
d) Traditional penal laws do not apply
e) Enacted legislations are neither keeping pace with changing technology nor harmonized
f) Cybercrime statistics are not accurate; many go undetected and unreported for various reasons.
g) Costly to develop and maintain security and other preventative measures.

CONCLUSION

Cybersecurity and cybercrime are intertwined issues that cannot be separated. Enhancing Cybersecurity and protecting key information infrastructure are essential to each nation's national security and economic

development. It is therefore necessary and prudent to ensure the harmonization of laws relating to cybercrime. This is informed by the fact that the legal, technical and institutional challenges posed by the issue of Cybersecurity are global and far-reaching. It can only be addressed through a coherent strategy taking into account the role of different stakeholders and existing initiatives, within a framework of international cooperation (Ghernouti-hélie, 2010).

Multi-national international organizations like the International Criminal Police Organization (Interpol), International Telecommunication Union (ITU), African Union, Council of Europe, the Commonwealth of Nations, the Group of 8 and the Organization for Economic Co-operation and Development (OECD), play pivotal roles in addressing cybercrime and their work encompasses a broader territorial environment. The Interpol has also provided technical guidance in cybercrime detection, investigation and evidence collection. The enactment of the Council of Europe's Convention on Cybercrime ("COECC") is also lauded because it attempts to establish consistency in the cybercrime laws of many countries. However, many states still have to sign and ratify the Convention to serve as a deterrent.

The reviewed literature on existing legislation indicates that though efforts are in place to bring about effective Cybersecurity regulation and policy, a lot of ground still remains uncovered. The issue of governing the multidimensional virtual world is rather complex, as it is not easy to define the territory and remains a major challenge. The Cybersecurity landscape continues to rapidly change and evolve. It is critical for policy makers to keep pace of these advancements with responsive and responsible legislative solutions. However, legislation alone can not solve threats posed to cyber world. It is therefore paramount to improve the capacity of human resources, strengthen collaboration within the national and international frontiers and consolidate the available prospects for modernity and the efficacy of the digital age.

REFERENCES

Bargh, M., Choenni, S., Mulder, I. and Pastoor, R. 2012. Exploring a warrior paradigm to design out cybercrime.

Berman, S.J. 2014. Digital transformation : opportunities to create new business models. Strategy and Leadership, 40(2):16–24.

Cassim, F. 2010. Addressing the challenges posed by cybercrime : A S. African perspective, 53:118–123.

Cerezo, A., Lopez, J. & Patel, A. 2007. International coop to fight transnational cybercrime, Wdfia.

Cheng, F. 2011. The Law Enforcement in Cyberspace Criminal focusing on the experience between Taiwan and the United States.

Craig Rosewarne. 2012. 2012/3 The South Africa Cyber Threat Barometer.

Ghernouti-hélie, S. 2010. A national strategy for effective cybersecurity approach and culture p. 370–373.

Government of Kenya Cybersecurity Strategy. 2014.

Grace Githaiga. 2013. A Report of the Online Debate on Africa Union Convention on Cybersecurity.

ICSPA. n.d.. The International cyber Security Protection Alliance.

Jang, Y.J., and Lim, B.Y. 2013. Harmonization among National Cyber Security and Cybercrime Response Organizations : New Challenges of Cybercrime.

Judge, and Schjolberg, S. 2014. Cybercrime Law.

Kharouni, L. 2013. Africa: A New Safe Harbor for Cybercriminals?

Kritzinger, E., and Solms, S. 2013. A Framework for Cyber Security in Africa. Journal of Information Assurance and Cybersecurity, 2012:1–10.

Lankshear, C., and Knobel, M. 2008. Digital literacies: concepts, policies and practices.

Liu, D.Y., Chen, S.-W., and Chou, T.C. 2013. Resource fit in digital transformation. Management Decision, 4910:1728–1742.

Marcum, D. 2014. The Digital Transformation of Information, Education, and Scholarship. International Journal of Humanities and Arts Computing, 8supplement, 1–11.

Marra, G. 2010. Controlled access to the internet, prevention of illicit uses and fundamental rights: A criminal law experience in light of the Italian "google case." Proceedings - 2nd International Conference on Evolving Internet, Internet 2010, 1st International Conference on Access Networks, Services and Technologies, Access 2010, 210–214.

McCombie, S., and Pieprzyk, J. 2010. Winning the phishing war: A strategy for Australia. Proceedings - 2nd Cybercrime and Trustworthy Computing Workshop, CTC 2010, 79–86.

Mesko, G., and Bernik, I. 2011. Cybercrime : Awareness and Fear Slovenian Perspectives.

Nambiro, A., Muchiri, G. and M. 2014. Cyber Security Assessment Framework: Case of Government Ministries in Kenya. International J. Technology in Computer Science and Engineering, 13:100-113.

Neufeld, D.J. 2012. Cybercrime Understanding Cybercrime :, 1–10.

Oluwafemi, O., Adesuyi, F. A., and Abdulhamid, S. M. 2013. Combating Terrorism with Cybersecurity : The Nigerian Perspective, 14, 103–109.

Phillips, A. 2011. E-Evidence and International Jurisdictions : Creating Laws for the 21 st Century, 1–5.

Popa, M. 2010. Audit Process during Projects for Development of New Mobile IT Applications. Informatica Economica, 143:34–47.

Sánchez, Ó.A. n.d.. Global Cybersecurity Agenda.

Sarantinos, N., Al-Nemrat, A., and Naeem, U. 2013. Statistical Sampling Approach to Investigate Child Pornography Cases. 2013 Fourth Cybercrime and Trustworthy Computing Workshop, 22–29.

Schjolberg, S. 2008. The history of global harmonization on cybercrime legislation - The road to Geneva.

Tabansky, L. 2012. Cybercrime : A National Security Issue? Military and Strategic Affairs, 43:117–136.

Wamala, F. 2012. ITU National Cybersecurity Strategy Guide.