International Journal of Cyber Criminology
Vol 12 Issue 1 January – June 2018

Legislating against Cyber Crime in Southern African Development Community: Balancing International Standards with Country-Specific Specificities

Lewis C. Bande[1]
University of Malawi, Malawi / KU Leuven, Belgium

Abstract
The growing threat of cyber crime has prompted a global call for countries to enact domestic cyber crime legislations as the first step in the fight against the vice. The predominantly transnational nature of cyber crime requires that domestic legislation must be harmonized in order to eliminate cyber crime safe havens and facilitate effective international cooperation. Simultaneously, it is imperative that such legislation must be diversified in order to address and incorporate country-specific challenges and needs. Balancing the competing needs for harmonization and diversification is, therefore, one of the major challenges when enacting domestic cyber crime legislations. This three-part article investigates whether, and to what extent, the legislations of three select countries of the Southern African Development Community (i.e., Botswana's Cyber crime and Computer Related Crimes Act, Tanzania's Cyber crimes Act and Malawi's Electronic Transactions and Cyber security Act) are balancing the two needs. This article examines the substantive law provisions of the three legislations, particularly the cyber crime offences against the confidentiality, integrity and availability of computers systems and data.

Keywords: Southern African Development Community, Cyber crime, Harmonization, Diversification, Budapest Convention.

Introduction

Increased usage of modern information and communication technologies (ICTs) in the Southern African Development Community (SADC) has made cyber crime a growing crime problem in the region. This has prompted regional-level and country-level efforts to tackle the problem by, *inter alia,* adopting cyber crime-related legislations. Thus, at regional level, SADC adopted the SADC Model Law on Cyber crime in 2012 to guide and facilitate the harmonization of domestic laws on cyber crime. At country level, as of July, 2017, nearly all member states of the grouping had enacted, or were in the process of enacting, cyber crime-related legislation.

[1] Lecturer in Law, Department of Foundation Law, Faculty of Law, University of Malawi; Doctoral scholar, KU Leuven, Belgium. Email: lewcbande@yahoo.com

As is the case with other countries worldwide that are enacting cyber crime legislations, SADC countries face a daunting balancing dilemma: how do they harmonize their domestic legislations with international standards whilst at the same time ensuring that such legislations are responsive to country-specific needs, challenges and realities? Harmonization is an indispensable prerequisite to international cooperation in the fight against transnational crime problems of the nature of cyber crime. However, there are still country-specific specificities that have to be addressed if legislation is to be effective and enforceable locally.

The goal of the article is two-tiered: firstly, it examines whether, and to what extent, the legislations of three SADC countries (i.e., Botswana's Cyber crime and Computer Related Crimes Act (No. 22 of 2007), Tanzania's Cyber Crimes Act (No. 4 of 2015) and Malawi's Electronic Transactions and Cyber Security Act (No. 11 of 2016) are harmonized with international standards, particularly those prescribed by the Council of Europe's Cybercrime Convention (the Budapest Convention). Secondly, it examines the extent to which the legislations are diversified to address country-specific specificities.

1. Balancing Harmonization and Divergence in Cyber Crime Legislations

1.1. Need for, and efforts at, international harmonization of cyber crime laws

Owing to the global nature and reach of the Internet, cyber crimes are "inherently transnational". The perpetrator may be located in one country whilst the victimized person, computer system or data is located in another country. Perpetrators may also use computer systems or networks in other countries as an attack base (what is called "remote attacks") or as a route to reach their victims. As a result, the perpetrators, victims, tools and scene of cyber crime are often transnational. It follows that the detection of cyber crimes, identification of perpetrators, the gathering of the necessary evidence and the prosecution of suspected cyber criminals often require the cooperation of authorities from multiple jurisdictions. Harmonization of cyber crime legislations is hailed as the first step towards effective international cooperation against cyber crime. In fact, international cooperation and harmonization are indispensable components in any strategy against cyber crime. Further, harmonization helps to eliminate "cyber crime safe havens" (Brenner & JJ Schwerha, 2008).

Efforts at harmonization have been organized at international and regional levels. Works by Li (2007), Schjolberg (2014) and others outlines in detail these efforts, and a summary overview should suffice here. At international level, the Budapest Convention is, to date, the only multilateral binding instrument on cyber crime. Its goal is to facilitate the harmonization of cyber crime legislations amongst its state parties. Though adopted under the aegis of the Council of Europe, its preparation involved other non-European countries, for instance, the United States, Japan and South Africa (Keller, 2011). And amongst its current 49 ratifications, 9 are non-European countries from around the world. It is the closest instrument to a global treaty on cyber crime.

Regionally, nearly all regional groupings have either binding instruments or model laws on cyber crime, adopted to facilitate the harmonization of cyber crime legislation. The African Union adopted the African Union's Convention on Cyber Security and Personal Data Protection in July, 2014; the European Union's adopted its Directive 2013/40/EU on Attacks Against Information Systems on 12 August, 2013; the League of Arab States

adopted the Convention on Combating Information Technology Offences in 2010; the Association of Southeast Asian Nations has the e-ASEAN Framework Agreement adopted in November 2013; whilst the Organization of American States has the Comprehensive Inter-American Strategy to Combat Threats to Cyber Security of 2004. Within Africa, at a sub-regional level, SADC has the SADC Model Law on Cybercrime and Computer Crime, whilst the Economic Commission for West African States has the Directive on Fighting Cyber Crime of 2011. All these international and regional efforts underscore the important countries worldwide attach to the need for harmonization.

1.2. The Budapest Convention as an Instrument for Global Harmonization

Cyber crime differs from other transnational crime problems because of its global nature. To effectively tackle it, what is needed is global harmonization and cooperation, and not only regional-level harmonization and cooperation. As rightly observed by Broadhurst, "the fight against cyber-crime either is a global one or it makes no sense" (Broadhurst, 2006). Moreover, with multiple regional-level instruments, there is a real danger that different instruments would prescribe different harmonization standards for their respective member states. This would frustrate efforts at global cooperation, what other authors have termed the "fragmentation of international responses" to cyber crime (Kasper, 2014). This may also result into "regional clusters" of harmonization and cooperation, involving countries within specific regions (Kastner & Megret, 2015).Faced with a global crime problem like that of cyber crime, what is needed is global cooperation. SADC countries must, therefore, strive to harmonize their legislations with global standards so that they are able to cooperate with countries worldwide.

The Budapest Convention is the closest instrument to a global treaty on cyber crime. In order to achieve broader harmonization beyond the African or SADC regions, we recommend that SADC countries must strive to harmonize their legislations with its standards. There are several reasons for this: the first is that, as already noted above, the Budapest Convention has the widest support than any cyber crime instrument to date. SADC's own Mauritius is actually a member, whilst South Africa, another SADC member state, is a signatory. The US, a leading country in the fight against, is also a member. The international membership of the Convention is likely to rise as the countries of Argentina, Chile, Colombia, Costa Rica, Mexico, Morocco, Paraguay, Peru, Philippines, Senegal and Tonga have been invited to accede.

The second reason is that some SADC countries have already used the Budapest Convention as a model for developing their domestic legislations on cyber crime. The legislations of Mauritius, Botswana and Tanzania, and the draft legislations of Lesotho and South Africa are clearly premised on the Convention. Furthermore, the SADC Model Law on Computer Crime and Cyber Crime is also modeled on the Budapest Convention.

Thirdly, the Budapest Convention has had broader acceptance and influence beyond its member states. For instance, a study by the United Nations Office on Drugs and Crime (UNODC) shows that, by the year 2014, 73 per cent of the responding countries worldwide had used the Convention for the development of their domestic legislation (UNODC, 2014). And the Commonwealth Group of Nations—one of the world's largest groupings of states with 53 member states—not only has its model law modeled on the Convention (Gillespie, 2014), but also encourages its member states to ratify it (Commonwealth, 2014). This attests to the global influence of the Budapest Convention. Consequently, if SADC countries were to harmonize their legislations with the

Convention, they will also have their legislations harmonized with those of seventy-five percent of the world's other countries. This means that it should be easier to cooperate with those other countries.

Of course the Budapest Convention does not enjoy universal support and has had a fair share of criticism. There is a clique of countries led by China and Russia that reject the Convention preferring instead a United Nations-backed instrument (Gillespie, 2014). Other countries, notably Russia, have also had sovereignty concerns over the Convention's article 32 that raises the possibility for trans-border access to data without the authorization of public authorities in the country where the data is being stored (Radziwill, 2016). It has further been criticized for being outdated, having been overtaken by technological and cyber crime developments that have occurred since its adoption in 2001 (Hauck &I, 2016). Nevertheless, the Convention is the best there is and since it only provides for minimum standards, some of its defects can be cured through the process of diversification being discussed below.

The Budapest Convention employs what is called the "minimum harmonization model". Under this model, countries harmonize their legislation by incorporating prescribed "minimum standards" and are allowed to go beyond the minimum by adopting additional "stricter or more far-reaching standards" (Vos, 2001). Minimum harmonization sets the mandatory minimum and affords countries a margin of appreciation. Hence, in pursuance of this model, the Budapest Convention only prescribes the minimum requirements and allows countries to adopt stricter and far-reaching legislations based on their challenges, needs and realities.

1.3. Need for Divergence

Besides harmonization, there is also a competing need for countries to ensure that their cyber crime legislations are responsive to country-specific and regional-specific realities and needs (International Telecommunication Union, 2012).This has been called the "glocal approach", whereby countries adopt "global initiatives and balancing them with local circumstances" (Chang, 2012). This is particularly important because most of the current international standard-setting instruments, particularly the Budapest Convention, were adopted by developed countries from the Global North and, hence, may not reflect the needs, realities and challenges prevailing in developing countries (International Telecommunication Union, 2012).

The need for divergence is also supported by the minimum harmonization model used by the Budapest Convention, whereby participating countries are permitted to go beyond the prescribed minimum by adopting additional "stricter or more far-reaching standards" depending on country-specific needs. The challenge, therefore, is on how to draw a healthy balance between harmonization on the one hand and the need to address country-specific needs on the other. The same is the challenge that SADC countries face.

2. Substantive Cyber Crime Offences

For substantive offences, minimum harmonization involves two things: the first is the conduct to be criminalized. Countries are required to criminalize certain minimum offences, and are allowed to add on these offences. The second is the definitional elements of the offences. The offences should have certain minimum definitional elements. There is also the overall need for clarity in the definition of the offences. It is important that

countries must draft their cyber crime legislations with sufficient clarity and specificity so as to ensure that they provide adequate foreseeability and guidance on the type of conduct being criminalized.

The Budapest Convention uses a typology that puts cyber crimes into four broad types: the first involves "offences against the confidentiality, integrity and availability of computer data and systems"; the second are "computer-related offences"; the third are "content-related offences"; and the third are "offences related to infringements of copyright and related rights."

2.1. Offences against the Confidentiality, Integrity and Availability of Computer Data and Systems

These offences penalize activities that target and compromise the confidentiality, integrity and availability of computer data and systems. A common denominator underlying these offences is that they have been made possible by networked computer technologies themselves. Consequently, they have been referred to as "true cyber crimes" (Clough, 2015) or "true cyber crimes" (Wall, 2007).The Budapest Convention has five of these offences: illegal access to computer systems (article 2); illegal interception of data (article 3); data interference (article 4); system interference (article 5); and misuse of devices (article 6).These are the minimum offences under this category of cyber crimes.

(i) Illegal access to computer systems

Commonly known as "hacking", the offence of illegal access to computer systems is one of the commonest of all cyber crimes. The core element of the offence is the unauthorized access of a computer system. It is analogous to offences of criminal trespass and breaking into a building in the real-world criminality. It has, thus, been referred to as "electronic trespassing" (Thomas, 2002) or "virtual breaking and entering" (Cross, 2008). The motivation for hacking differs: others hack for fun, others to send a political message (the so-called "hacktivists"), whilst others hack as a gateway to other offences, for instance, website defacement, data theft, fraud and others. Whatever the motivation, hacking is criminalized because it violates the confidentiality and integrity of computer systems.

Article 2 of the Budapest Convention describes the criminalized conduct as "access to the whole or any part of a computer system without right". A domestic law transposing that article needs to have, at a minimum, four definitional elements: the first and basic element is "access" to a computer system. The term "access" is explained in the Explanatory Report to the Budapest Convention (Explanatory Report) as meaning the entering of the whole or any part of a computer system. The definition is wide and open-ended, covering all means of entering computer systems as made possible by existing and future technologies. Secondly, what is accessed must be to a "computer system", a phrase that is defined in the Budapest Convention as meaning "any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data" (Article 2). It may have input, output, and storage facilities, and may stand alone or be connected in a network with other computer systems.

The third element is that access must be "without right," which basically means without legal authority, or any other access that is not covered by established legal defenses as they are available in a country's domestic law (for instance, the defenses of duress, self-defense or mistake of fact) (Explanatory Report, para. 38). This means that the criminalization need not extend to access done with the consent of the owner of the computer system, or access by a member of the law enforcement agency done in

pursuance of a court order. The fourth and last element is that the illegal access must be intentional. The principles governing intention as a form of *mens rea* in a country's legal system apply. The Convention grants countries the discretion to restrict the criminalization to instances when illegal access is obtained through an infringement of security measures, or where the hacker acted with an ulterior motive of obtaining computer data, or had some other "dishonest intent." However, a definition that incorporates the four elements satisfies the standards of the Convention.

The legislations of all the three SADC countries criminalize illegal access to a computer system. Botswana's Cyber Crime and Computer Related Crimes Act criminalize "unauthorized access to a computer or computer system" in its section 4. A person commits the offence if he or she either accesses the whole or any part of a computer or computer system, knowing that such access is unauthorized or causes a computer or computer system to perform any function as a result of unauthorized access to such system. The first type of conduct covers a typical illegal access to a computer system, whilst the second part expands the ambit of the criminalization to include causing a computer system to perform any function after gaining unauthorized access. The term "access" is explained in the statute as meaning to "instruct, communicate with, store data in, retrieve data from, or otherwise make use of any of the resources of the computer or computer system" (section 2). That definition is wide, and covers the initial entering of a computer system as well as subsequent acts, for instance, storing and retrieving data, or using the resources of a computer. It follows that a person who has the authorization to enter a computer system, but has no authorization to store or retrieve data from the computer system, would commit the offence if he or she stores data in, or retrieves data from, the computer system. It also means that merely instructing or communicating with a computer system, without actual entry into the system, amounts to an offence under the section. That definition is wide, and covers basic unauthorized entry into a computer system (as envisaged by the Budapest Convention), as well as other activities such as instructing a computer system, communicating with a computer system, storing and retrieving data from a computer system, as well as using the resources of the computer system. Such extensions are allowed under the minimum harmonization model employed by the Convention, since they are within the philosophy of the criminalization. As for the mental element, the person must have acted with knowledge that the access is unauthorized. Under Botswana's general criminal law, knowledge necessary to establish criminal liability involves either "actual knowledge" or "wilful blindness" (Nsereko, 2011).

Tanzania's Cyber Crimes Act defines the offence of illegal access in its section 4, which states that a "person shall not intentionally and unlawfully access or cause a computer system to be accessed." A person commits the offence by either accessing a computer system, or causing a computer system to be accessed by another person. The second part covers those who enable or facilitate the commission of the offence. The term "access" is defined as meaning "entry to, instruct, communicate with, store data in, retrieve data from, or otherwise make use of any of the resources of the computer system or network or data storage medium" (section 2). As is the case with Botswana's definition, the term access has been broadly defined to include initial entering of a computer system, as well as conduct done whilst access is gained. A person who has authority to enter a computer system, but stores data in, retrieves data from, or otherwise makes use of the resources of

the computer system without authority, would also commit the offence. An important definitional element is that the access must be "unlawful," which basically means that it must be contrary to any law. Hence, access without the express or implied permission of the owner or controller of a computer system is unlawful. In terms of applicable mental element, the person must act with the intention of gaining unlawful access to a computer system.

Malawi's Electronic Transactions and Cyber Security Act define the offence of "hacking" under its section 92. The relevant part of that section states that: "Any person who hacks into any computer system…commits an offence." There is no statutory definition of the term "hack". One, therefore, has to have recourse to ordinary grammatical meaning of that term and, ordinarily, hacking means to gain unauthorized access of a computer system. Unlike Botswana's and Tanzania's definition, the criminalization under Malawi's statute is limited to the basic unauthorized entry into a computer system. The use of the technical term "hack" in the definition of the prohibited conduct violates one of the best practices in the drafting of cyber crime legislations, viz., that as much as possible, and whilst not compromising on the clarity of the law, "technology–neutral language" must be preferred when defining cyber crime offences (Downing, 2004). This is necessary to ensure that the criminalization covers both existing and future technologies. A "computer system" is defined as meaning "a device or a group of interconnected or related devices, one or more of which performs automatic processing of data pursuant to a program" (section 2). That definition corresponds with the definition under the Convention. Another major shortfall in the definition is that no mental element is specified in the section. In practice, this should be remedied by the principle of Malawian criminal law that *mens rea* must be presumed to apply in every offence, unless expressly or impliedly displaced by a statute (Bande, 2017). The wording of section 92 cannot be said to displace that presumption, and *mens rea* in the form of at least knowledge must be read into the provision.

(ii) Illegal Interception of Computer Data

The second offence against the confidentiality, integrity and availability of computer data and systems is that of "illegal interception", which is provided under article 3. An interception happens to data during its transmission either between or within computer systems. The equivalent of this type of conduct in the offline criminality is telephone wiretapping and eavesdropping.

Article 3 of the Budapest Convention requires countries to criminalize: "the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data." The interception must be done intentionally. A number of elements are identifiable. The first and core definitional element of the offence is that there must be an "interception" of a transmission of computer data. The term "interception" has been defined as covering a range of activities, including recording data, listening to or monitoring the content of communications, procuring the content of data either directly (i.e., through access and use of the computer system) or indirectly (i.e., through the use of electronic eavesdropping or tapping devices) (Explanatory Report, para 53). The interception must be done to data during its "transmission", a term that covers all data transfers, whether by telephone, fax, e-mail or

file transfer (Explanatory Report, para. 53). The transmission can be to, from or within a computer system.

The third element is that the interception must be "by technical means," which in effect excludes from the criminalization any interception by non-technical means. It has been observed that this requirement is redundant, because "interceptions in the digital environment can be achieved exclusively by using technical means" (Vasilescu, 2015). However, its use was justified as a "restrictive qualification to avoid over-criminalization" (Explanatory Report, para. 53). The fourth element is that the offence targets the interception of "non-public transmissions of computer data" only. The "non-public transmission" qualifies the nature of the transmission, and not the nature of the data being transmitted (Explanatory Report, para. 54). In other words, a transmission is "non-public" if the parties involved in the transmission intend it to be private, even if the content of the transmission is public knowledge. This underscores the fact that it is the privacy of the transmission that is sought to be protected by the criminalization. The interception must also be "without right," and must be "intentionally."

Article 3 has left it to the parties to decide whether to require that the offence must be committed with some "dishonest intent" or to require that the offence can only be committed against a computer system that is connected to another computer system.

For Botswana, section 9 of its Cyber Crime and Computer Related Crimes Act makes it an offence for any person to intercept (a) any non-public transmission to, from or within a computer or computer system; or (b) electromagnetic emissions that are carrying data, from a computer or computer system. The person must act "intentionally", "by technical means" and "without lawful excuse or justification". The definition incorporates all the key definitional elements of the offence of data interception as prescribed by the Budapest Convention. It requires that there must be an interception, through technical means, of a non-public transmission of computer data to, from or within a computer or computer system. It further covers the interception of electromagnetic emission from a computer system. In short, the definition is in all fours with the Budapest Convention's minimum requirements

On its part, section 6 of Tanzania's Cyber Crimes Act makes it an offence for any person to intercept by technical means or by any other means (i) a non-public transmission to, from or within a computer system; (ii) a non-public electromagnetic emission from a computer system; (iii) a non-public computer system that is connected to another computer system. The interception must be "intentionally and unlawfully". For a start, section 2 to that Act defines the term "interception" as including "acquiring, viewing, listening or recording any computer data communication through any other means of electronic or other means, during transmission through the use of any technical device." Whilst the wording of definition should have been improved, it nevertheless captures the essence of interception as envisioned in the Budapest Convention. Further, the definition emphasizes that the interception must be by technical means. Further, what must be intercepted is a non-public transmission of computer data, during transmission to, from or within a computer system, as well as electromagnetic emissions from a computer system. Surprisingly, the criminalization also covers the interception of "non-public computer system that is connected to another computer system." This was an unnecessary addition because such an interception is covered by paragraph (a).

Under Malawi's Electronic Transactions and Cyber Security Act, the prohibition against data interception is contained in section 87(3), which punishes any person who "intercepts any data without authority or permission to do so." There is no statutory definition of the term "intercept" and, hence, the ordinary meaning of that term applies. Hence, the criminalization covers recording, listening to or monitoring of the content of a computer communication, as well as the procuring of the content of data. The interception must be done to data during its transmission to, from, and within a computer system. It is expressly required that the interception must be without authority or permission, and intentional. Malawi's definition is unnecessarily skeletal and basic. The definition would have been improved by merely looking at how other countries both regionally and internationally have drafted their own offences on data interference. Moreover, the requirement that the interception must be to non-public transmission of data has not been included, and omission that renders the offence overly broad.

(iii) Data Interference

In a digitized world in which we live, computer data has become not only indispensable but also extremely valuable to individuals, organizations and governments. Damage to data can be costly. Just as the general criminal law punishes any damage to traditional forms of property (for instance, through the offences of criminal damage and arson), so too do cyber crime laws seek to punish any malicious damage to data through the offence of "data interference". A key difference between "data interception" and "data interference" is that the former affects data during the transfer process, whilst the latter affects data during its storage.

Article 4 of the Budapest Convention recommends for the criminalization of "the damaging, deletion, deterioration, alteration or suppression of computer data without right." This must be done intentionally. Damaging, deleting, deteriorating, altering and suppressing data are the several ways how data may be interfered with, thereby compromising its integrity and availability. The terms "damaging" and "deteriorating" are said to be overlapping acts, and pertain to the negative alteration of the integrity of the data (Explanatory Report, para. 61). On the other hand, "deletion" involves the actual destruction of the data and renders them unrecognizable (Explanatory Report, para. 61). "Suppressing" covers any action that prevents the availability of the data to legitimate users of the computer system where it is stored. Lastly, "alteration" involves any modification of existing data (Explanatory Report, para. 61). The commonest way of committing data interference involves the introduction of malicious codes, such as viruses and Trojan horses. As is the case with other offences under the Convention, to amount to an offence, the interference must be both without right and intentional.

The Convention has left it to the countries to limit the criminalization to conduct that occasions "serious harm" only (article 4(2)). Such a limitation has parallels in the offline world, where criminalization of damage to property is often subject to the *de minimis* principle.

Botswana's Cyber Crime and Computer Related Crimes Act provides for data interference under its section 7, which seeks to punish any person who either destroys, deletes, suppresses, alters or modifies data or renders data meaningless, useless or ineffective. To be liable, the person must act "intentionally" and "without lawful excuse or justification." The section covers the basic elements of the offence as prescribed by the Budapest Convention.

On its part, section 7 of Tanzania's Cyber Crimes Act makes it an offence for any person who (a) damages or deteriorates computer data; (b) deletes computer data; (c) alters computer data; (d) renders computer data meaningless, useless or ineffective. The person commits the offence if he or she acts intentionally and unlawfully. The word unlawful should be interpreted as meaning without lawful excuse or justification. The definition also captures the elements of the offence as required by the Budapest Convention.

And section 87(4) of Malawi's Electronic Transactions and Cyber Security Act punishes any person who "interferes with data in a way which causes such data to be modified, destroyed or otherwise rendered ineffective." The person must act "intentionally and without authority to do so". Although the definition could have been further improved by expressly listing the various activities that would interference with data, Malawi's definition satisfies the minimum requirements under the Convention.

(iv) Systems Interference

Computer data, because of its digital nature, exist and function within computer systems. The legal protection of such data would be ineffective if the computer systems themselves are also not protected. That is why cyber crime laws also seek to punish any interference with the proper functioning of computer systems.

Article 5 of the Budapest Convention provides for the minimum requirements for the offence of "systems interference". It requires countries to criminalize "the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data." The offence must be committed intentionally. A number of elements are identifiable from that article. The first and primary element of the offence is that the activity must involve the "hindering" of the functioning of a computer system. The term "hindering" has been explained as referring to any action that interfere with the proper functioning of the computer system (Explanatory Report, para. 66).

The second element has a limiting effect, as it requires that the hindering must be occasioned by the "inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data." Other acts of system interference have been excluded from the criminalization. Typical examples of committing the offence include denial of service attacks, sending malicious codes such as viruses that interfere with the operation of the system, or programs that send huge quantities of spam that block the communications functions of the system (Explanatory Report, para. 67). In effect, therefore, the criminalization targets any interference with the functioning of a computer system occasioned by data interference. Another limiting element is that the hindering must be "serious." The Convention has left it to countries to decide what hindering qualifies as "serious" (Explanatory Report, para. 67).The offender must have acted intentionally (i.e., with "the intent to seriously hinder" (Explanatory Report, para. 78) and "without right."

Section 8 of Botswana's Cybercrime and Computer Related Crimes Act punishes any person who either hinders or interferes with the functioning of a computer or computer system or hinders or interferes with a person who is lawfully using or operating a computer or computer system. To be liable, the person must act "intentionally" and "without lawful excuse or justification". Section 8(2) explains the term "hinder" as including cutting electricity supply to a computer or computer system; causing electromagnetic interference to a computer or computer system; corrupting a computer or

computer system by any means; inputting, deleting, altering or modifying data; and impairing the connectivity, infrastructure or support of a computer or computer system. Anyone of these amounts to a hindering. What is interesting about this explanation is that it includes an offline conduct of cutting electricity supply to a computer or computer system. What is clear, however, is that the legislature in Botswana intended to cast the ambit of criminalization wide, by capturing all acts of interference with computers and computer systems. The criminalization is therefore wider than one recommended by the Budapest Convention, which is limited to interference caused by the "inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data."

Further, the criminalization also targets hindering or interfering with a person who is lawfully using or operating a computer or computer system. It is not clear whether such a hindrance or interference must be through technical or non-technical means. However, if one considers the meaning of the term "hinder" given in section 8(2), the hindrance must involve cutting electricity supply to the computer system, causing electromagnetic interference to a computer system, corrupting a computer system, inputting, deleting, altering or modifying data and impairing the connectivity, infrastructure or support of a computer or computer system. Any other form of interference or hindrance is not covered. Finally, the statute requires that the person must act intentionally and without "lawful excuse or justification."

For Tanzania's Cyber Crimes Act, "Illegal system interference" is provided for under section 9, which makes it an offence for any person to hinder or interfere with either the functioning of a computer system or the usage or operation of a computer system. The term "hinder" is further explained as including causing electromagnetic interference to a computer system; corrupting a computer system by any means; or inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data. By including the interference caused by electromagnetic interference and corrupting computer systems, the criminalization is wider than one recommended by the Convention, which is restricted to interference caused by the "inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data."

Malawi's Electronic Transactions and Cyber Security Act have two offences relating to system interference. The first is provided for under section 87(8)(b), which seeks to punish any person who "introduces or spreads a software code that damages a computer, computer system or network." The criminalization under that section is limited to the introduction and spreading of malicious codes that damages a computer or computer system. In computing terminology, a "malicious code" is essentially a computer program that, once it gets into a computer, damages or disrupts its resources, including files, programs and system software. Common examples of such codes are viruses, worms, Trojan horses, logic bombs, bots, root kits and back doors.

The second offence is provided for under section 93, which punishes "any person who wilfully or maliciously renders a computer system incapable of providing normal services to its legitimate users." Anything that renders a computer system incapable of providing normal services to legitimate users is covered. A literal reading of the provision would include both technical and non-technical activities. In practice, however, most activities that would hinder a computer system from providing normal services would be technical in nature. The criminalization is also not limited to an interference caused by the inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data as required under the Budapest Convention.

Malawi's two offences should have been combined into one, because they target various modes of interfering with a computer's system. Malware interferes with computer systems. Similarly, the criminalization under article 93 targets one aspect of systems interference (i.e., rendering a computer system incapable of providing normal services). The best approach for Malawi was to enact a single offence of system interference, which would capture the various ways of committing that offence.

(v) Misuse of Devices

To commit the offences of illegal access, data interception, data interference or system interference often requires the use of certain technical tools, what are commonly referred to as "tools of cyber crime" or "hacker tools" (Kizza, 2014). These are computer programs, passwords, access code or other devices that can be used to commit cyber crimes. The offence of "misuse of devices" seeks to punish those who trade, deal in, make available or even possess these tools of cyber crime. Even in traditional real-world criminality, criminal laws across the world also punish those who trade in or supply instruments of crime. This is an ancillary offence to the offences discussed above.

Article 6 of the Budapest Convention calls for the criminalization of two types of activities: firstly, "the production, sale, procurement for use, import, distribution or otherwise making available of a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5." Each one of these (i.e., the mere production, selling, procuring for use, importation, distribution) constitute the various ways of committing an offence.

It is important to emphasize that the device must be "objectively designed, or adapted, primarily for the purpose of committing an offence" (Explanatory Report, para. 73). This means that the criminalization does not apply to "dual-use devices" (i.e., devices capable of being used for both lawful and unlawful purposes).However, by limiting the offence to devices that are objectively designed or adapted primarily for criminal purposes, the offence does not seek to punish legitimate dual-use devices, and other devices developed by researchers and other professional working in computer security. Hence, devices developed for the purposes of authorized testing or protection of computer systems are not covered by the criminalization.

Secondly, the article recommends the criminalization of the production, sale, procurement for use, importation, distribution or otherwise making available of "a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5." Thirdly, the article requires the criminalization of the possession of such a device or computer password, access code or similar data, where such possession is accompanied by the intent that it be used for the purposes of committing the offences under article 2 through 5. It is a requirement that the offence must be "committed intentionally and without right".

All the three countries have offences that criminalize misuse of devices. For Botswana's Cyber Crime and Computer Relates Crimes Act, the relevant provision is section 10, which criminalizes a number of activities as follows: firstly, it punishes any "person who intentionally, without lawful excuse or justification, manufactures, sells, procures for use, imports, exports, distributes or otherwise makes available, a computer or computer system

or any other device, designed or adapted for the purpose of committing an offence under this Act" (article 10(1)). The wording of the section gives one the impression that the devise need not be designed or adapted primarily for the purposes of committing cyber crimes, and that dual-use devices are covered. However, the requirement that the person must act "without lawful excuse or justification" saves the day, as dealing in such dual-use devices for non-criminal and legitimate purposes would not be "without lawful excuse or justification". Similarly, dealing in devices that are primarily designed or adapted for committing offences but for some other lawful reason (for instance, testing security systems of computer systems or networks) is also not covered by the criminalization. However, we are of the view that the section should have included a requirement that the person must act with the specific intent of committing an offence. Secondly, section 10(2) targets any "person who intentionally, without lawful excuse or justification, receives, or is in possession of, one or more of the devices under subsection (1)" (article 10(2)). The targeted conduct under this subsection consists of either receiving or possession of any device designed or adapted for the purpose of committing an offence. Such receiving or possessing must be without lawful excuse or justification, which means that receiving or possessing such a device for some lawful use is not covered. Thirdly, under section 10(3), any "person who is found in possession of any data or programme with the intention that the data or programme be used, by the person himself or herself or by another person, to commit or facilitate the commission of an offence under this Act", the subsection targets those who are found in possession of computer data or programme, with the specific intention of using them to commit or facilitate the commission of an offence under that statute. That actual intention must be objectively proved, and not merely inferred from the act of possession.

Tanzania's Cyber Crimes Act states, in its section 10, criminalizes dealing with or possession of (a) a device, including a computer program, that is designed or adapted for the purposes of committing an offence; (b) a computer password, access code or similar data by which the whole or any part of a computer system if capable of being accessed with the intent that it be used by any person for the purpose of committing an offence. A person must act "unlawfully." The first part of the section risks *over*-criminalization. The targeted conduct consists of dealing with or possessing a device that is designed or adapted to commit an offence. This includes dual-use devices. Unlike Botswana's definition, it is not a requirement that the person must act without lawful excuse or justification, meaning that any dealing with or possession suffices. The requirement that the person must act unlawfully does not help the matter, because it is not clear in what circumstances a mere dealing with or possession would be unlawful, unless Tanzania has a law that regulates the dealing with or possession of such devices. It should have been made clear in the definition that the person must deal with or possess the device without lawful excuse or justification, and that the device itself must be primarily designed or adapted to commit an offence. The second part of the definition (i.e., dealing with or possession of a computer password, access code or similar data by which the whole or any part of a computer system if capable of being accessed) has no problem with over-criminalization because it expressly requires that the person must act with the intent that it be used by any person for the purpose of committing an offence.

For Malawi, section 87(5) of the Electronic Transactions Act makes it an offence for any person to produce, sell, offer to sell, procure for use, design, adapt for use, distribute or possess any device or computer program, a component or a phone, which is designed

primarily to overcome security measures for the protection of data. Secondly, it also makes it an offence to produce, sell, offer to sell, procure for use, design, adapt for use, distribute or possess "a password, access code or any other similar kind of data with the intent to unlawfully utilizing such item."

The two offences have pertinent similarities and differences: under the first, what must be produced, sold, offered for sale, etc., must be any device, computer program or a phone. Secondly, such device must be primarily designed to overcome security measures for the protection of data. By limiting the criminalization to devices designed to overcome security measures for the protection of data, the offence does not apply to devices that can be used to commit other cyber crimes. This was an unnecessary limitation. The second criminalization targets the production, selling, etc., of passwords, access codes or similar data, but with intent to unlawfully use them. To commit the offence, the person must act with the intent to "unlawfully" utilize such item. Under Malawian criminal law, an act is said to be "unlawful" if it is contrary to the general law of the country, whether statutory law or common law, and whether civil law or criminal law. The criminalization should have been limited to passwords or access codes that can be used to commit only criminal offences. As regards the mental element, the section requires that the person must produce, sale, possess or distribute, etc., a device, computer program, password or access code "with the intent to unlawfully utilize such item". A subjective intention to unlawfully use the item must be proved before criminal liability is imposed.

(vi) Additional Offences in the Three Countries

The Budapest Convention only provide for the minimum offences against the confidentiality, integrity and availability of computer data and systems. Countries are at liberty to add on those offences, if the need be. Further, having been adopted in 2001, and considering the rapid changes in modern information and communication technologies, the Convention has been criticized that it is "outdated" (Jakobi, 2013). Particularly for the substantive offences, it has been noted that the Convention "is based on criminal cyber conducts in the late 1990s"(Schjolberg, 2014) and that it does not include the new forms of cyber crimes made possible by recent technological developments, for instance, social networks (Gillespie, 2016). Lastly, having been adopted by the developed European countries and the United States, the Convention has also been criticized for ignoring "the unique threats and concerns that developing nations face" (French, Wakefield, Brouse & Bragarnik, 2012). Such criticism is based on the assumption that developing countries face different cyber threats that are different from those faced by developed nations. So, have the three SADC countries added on the minimum core offences recommended by the Convention?

Botswana's Cybercrime and Computer Related Crimes Act has three additional offences aimed at protecting the confidentiality, integrity and availability of computer data and systems. The first offence is that of "unauthorized access to computer service", as provided for under its section 5. The offence punishes any person who "knowingly and by any means, without authorization or exceeding the authorization he or she is given (*a*) secures access to any computer or computer system for the purpose of obtaining, directly or indirectly, any computer service; or (*b*) intercepts or uses to be intercepted, directly or indirectly, any function of, or any data within, a computer or computer system." The offences under the two paragraphs are different: under paragraph (a), what is punished is

unauthorized access to a computer system "for the purposes of obtaining…a computer service." A "computer service" is defined as including "data processing or the storage or retrieval of data" (article 2). This is basically an extension of the offence of unauthorized access to a computer system under section 4 of that Act, but committed with the specific intent to obtain a computer service. Under paragraph (b), what is criminalized is the interception of a function or data within a computer or computer system. We are failing to see how this criminalization is different from that of unlawful interception of data under section 9 of the Cyber Crime and Computer Related Crimes Act.

The second additional offence is provided for under section 6, which defines the offence of "access with intent to commit an offence". A person commits the offence if he or she "with intent to commit an offence under any other enactment, causes a computer or computer system to perform any function for the purpose of securing access to-(*a*) any programme or data held in a computer or computer system; or (*b*) a computer service". The offence is also a subspecies of the offence of illegal access to a computer system as provided for under section 4, with the difference that the offence under section 6 is committed with a distinct motivation or intention to commit another offence. Under section 6(2), the access may be authorized or unauthorized.

The last additional offence is that of "unauthorized disclosure of a password" under section 11. It punishes any person "who intentionally, without lawful excuse or justification, discloses, sells, procures for use, distributes or otherwise makes available, any password, access code or other means of gaining access to the whole or part of a computer or computer system-(a) for wrongful gain; (b) for any unlawful purpose; (c) to overcome security measures for the protection of data; or (d) with the knowledge that it is likely to cause prejudice to any person." This offence compliments that of "misuse of devices" under section 10 of that Act. The difference between the two is that the offence under section 11 applies to passwords, access codes and other means of gaining access to the whole or any part of a computer system.

Tanzania's Cyber Crimes Act has two additional offences: the first is that of "illegal remaining" (section 5), and that of "data espionage" (section 8). Under the first offence, a person commits the offence if he or she intentionally and unlawfully remain in a computer system or continue to use a computer system after the expiration of time which he or she was allowed to access the computer system. The offence compliments that of "illegal access", which is provided under section 4, in the sense that it envisages a situation where the initial access was authorized but the person extends access after the withdrawal or expiry of the authorization. The Budapest Convention does not punish the offence of illegal remaining, but such an offence is included in the SADC Model Law on Computer Crime, which was adopted by SADC in order to facilitate the harmonization of cyber crime legislations in the region.

The offence of data espionage is defined as the obtaining of "computer data protected against unauthorized access without permission." The criminalized conduct consists of the acquisition or taking of data, and not mere access to data. This may involve copying such data or even downloading it. It is analogous to that of theft. The data must be protected against unauthorized access, meaning that the person must not have the right to access such data in the first place. The criminalization does not apply to publicly available data.

Malawi's Electronic Transactions and Cyber Security Act has four additional offences: the first is that of unauthorized access to data (section 87(3)), which is a distinct offence to that of unauthorized access to computer system. What is targeted is mere access to data,

whether access to the computer system where the data is accessed from is authorized or not. Where access to the computer system is not authorized, a person commits two offences, of unauthorized access to a computer system and unauthorized access to the data. Where access to a computer system is authorized, a person can still commit the offence of unauthorized access to data if he or she accesses data within that computer system he or she is not authorized to access.

The second is that of unauthorized communication, disclosure or transmission of data, information, program, access code or command to any person not entitled or authorized to access such data, information, program, code or command (section 87(8)(a). The offence does not only protect data but also "any…information, program, access code or command." The section does not qualify the protected data, information, program, access code or command as "computer data", "computer information", "computer program", "computer access code" and "computer command." Of course, being a cyber crime, one may argue that the provision is actually talking about data, information, program, access code and command relating to a computer.

The third additional offence is that of receiving computer data not entitled to (section 87(9)). The offence compliments that of unauthorized communication, disclosure or transmission of data, information, program, access code or command under section 87(8)(a). But the ambits of the two offences are surprisingly different: whilst section 87(8)(a) punishes a person who communicates, discloses or transmits data, information, program, access code or command without authorization and to a person not entitled thereto, section 87(9) is only limited to data. It does not punish the one who receives computer information, program, access code or program. The fourth offence is that of accessing or destroying files or information without authorization, or for the purposes of concealing information necessary for an investigation into the commission of an offence (section 87(8)(c)). There is a clear overlap between this offence and the offences of hacking and unauthorized access to data (both under section 87(3)) and data interference (under section 87(4). In the words, the offence is a clear redundancy. The last additional offence involves damaging, deleting, altering or suppressing any communication or data (article 87(8)(d)). Again this offence is redundant, as the targeted conduct is covered by the offence of data interference.

Conclusion

In general terms, the legislations of Botswana, Tanzania and Malawi incorporates the minimum requirements prescribed by the Budapest Convention relating to offences against the confidentiality, integrity and availability of computer systems and data. Whether intended by the legislatures of the three countries or by default, the harmonizing standards of the Convention have found their way into the legislations of the three countries. However, there is a need for fine tuning on some of the offences, particularly for Malawi's Electronic Transactions Act. It is important that the definition of offences must communicate clearly and precisely the conduct being criminalized and the applicable mental elements. The use of technical language in the definition of the prohibited conduct should also have been avoided.

There also has been an attempt to add on the core offences under the Convention in the three statutes. But this has involved broadening the offences, and not breaking new grounds in terms of new forms of criminality. This underscores the fact that it is difficult

for African countries to have completely novel cyber crimes against the confidentiality, integrity and availability of computer data and systems.

References

Bande, L. C. (2017). *Criminal Law in Malawi*. Cape Town: Juta.

Bassiouni, C. M. (1999). *Crimes Against Humanity in International Criminal Law*. The Hague: Kluwer Law International.

Barberet, R., & Joutsen, M. (2010). Crime and Justice. In Immerfall, S. & Therborn, G. (Eds.), *Handbook of European Societies: Social Transformations in the 21st Century* (pp. 139-155). New York, NY: Springer.

Beare, M. E. (2010). *Encyclopaedia of Transnational Crime and Justice*. Thousand Oakes, CA: SAGE.

Brenner, S. W. & Schwerha, J. J. (2007-2008). Cybercrime havens: Challenges and solutions. *Business Law Today, 17*(2), 49-79.

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing: International Journal of Police Strategies and Management, 29(3)*, 403.

Chang, L. Y. (2012). *Cybercrime in the Greater China Region: Regulatory Responses and Crime Prevention Across the Taiwan Strait*. Cheltenham: Edward Elgar.

Clough, J. (2015). *Principles of Cybercrimes*, Cambridge: Cambridge University Press.

Cross, M., & Shinder, D. (2008). *Scene of the Cybercrime* Burlington, MA: Syngress.

Downing, R. W. (2004-2005). Shoring up the weakest link: What lawmakers around the world need to consider in developing comprehensive laws to combat cybercrime. *Columbia Journal of Transnational Law, 43,* 704-762.

French, T., Wakefield, M., Brouse, K.,& Bragarnik, Y. (2012). Criminal Courts and Tribunals. *20*(1), *Human Rights Brief, 20*(1), *48-54.*

Ghernaouti, S. (2013). *Cyber Power: Crime, Conflict and Security in Cyberspace*. Burlington: EPFL Press.

Gillespie, A. A. (2016). *Cybercrime: Key Issues and Debates*. London: Routledge.

Hauck, P., & Peterke, S. (2016). *International Law and Transnational Organised Crime*. Oxford: Oxford University Press.

International Telecommunications Union (2012). *Understanding cybercrime: Phenomena, challenges and legal response*. Geneva: International Telecommunications Union.

Jakobi, A. P. (2013).*Common Goods and Evils? The Formation of Global Crime Governance*. Oxford: Oxford University Press.

Kasper, A. (2014). The Fragmented Securitization of Cyber Threats. In Kerikmäe, T. (Ed.), *Regulating eTechnologies in the European Union: Normative Realities and Trends* (pp. 157-193) Cham: Springer.

Kastner, P., & Megret, F. (2015). International legal dimensions of cybercrime. In Tsagourias, M. & Buchan, R. (Eds.), *Research Handbook on International Law and Cyberspace* (pp. 190-213) Cheltenham: Edward Elgar.

Keller, P. (2011). *European and International Media Law: Liberal Democracy, Trade, and the New Media*. Oxford: Oxford University Press.

Kizza, J. M. (2014). *Computer Network Security and Cyber Ethics*. Jefferson: Mcfarland.

Lohse, E. J. (2011). The meaning of harmonisation in the context of European Union law—a process in need of definition. In Andernas, M., & Andersen, C. (Eds.), *Theory and Practice of Harmonisation* (pp. 282–313). Cheltenham: Edward Elgar.

Nsereko, D. D. N. (2011). *Criminal Law in Botswana*. Deventer, Netherlands: Wolters Kluwer.

Schjolberg, J. (2014). *The History of Cybercrime: 1976–2014.* Norderstedt: Books on Demand.

Schütze, R. (2015).*European Union Law*.Cambridge: Cambridge University Press.

The Commonwealth "Report of the Commonwealth Working Group of Experts on Cybercrime" (May 2014) Retrieved from http://thecommonwealth.org/sites/default/files/news-items/documents/Report_of_the_Commonwealth_Working_Group_of_Experts_on_Cybercrime_May_2014.pdf.

Thomas, T. (2002). New Ways to Break the Law: Cybercrime and the Politics of Hacking. In Jewkes, Y. & Letherby, G. (Eds.), *Criminology: A Reader* (pp. 387-398)London: Sage.

United Nations Office on Drugs and Crime (2013). Comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector. Retrieved from https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_E.pdf.

Vasilescu, L. (2015). Illegal interception of computer data transmission in the regulation of the New Romanian Criminal Code. *Journal of Law and Administrative Sciences, 3*, 230-238.

Vos, E. (2001). Differentiation, Harmonisation and Governance. In de Witte, K., Hanf, D. & Vos, E. (Eds.), *The Many Faces of Differentiation in EU Law* (145). Antwerp: Intersentia.

Wall, D. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge: Policy.