CYBER CRIME LEGISLATION FUNDAMENTALS

Submitted as a Guidance towards the review of Zimbabwe's Cyber Crime Legislation

Arthur Gwagwa and Otto Saki

1. Introduction: Connectivity and cybercrime

Technology is moving so fast that society could soon feel the repercussions of the Fourth Industrial Revolution. In the hyper connected world of tomorrow, it will become hard to imagine a 'computer crime', and perhaps any crime, that does not involve electronic evidence linked with internet protocol (IP) connectivity. It is in this context that we present this report setting fundamentals of a cybercrime legislation to guide the review of Zimbabwe's Cyber Crime Bill. Instead of being prescriptive, we take a discursive approach. The guidelines we set out could have been more specific and brief if we were tailoring them to the actual bill. Nevertheless, we base this report on the Global baseline survey titled (the "Comprehensive study of cybercrime) commissioned by the UN Office on Drugs and Crime, co-authored by our colleague Joss Wright at Oxford University. We update the findings considering developments that have occurred since the said survey.

Key Finding: A cybercrime law should ideally contain the following essential elements: Core definition of cyber Crime based on confidentiality, Integrity and availability of computer related data; other criminalised acts related to computer misuse and content, law enforcement and investigations procedures, treatment of electronic evidence in criminal justice, international cooperation, such as mutual legal assistance (MLATs), cybercrime prevention and awareness raising. There should also be provision for computer response teams or computer emergency responses teams, protection of critical infrastructure, to avoid a separate Cybersecurity Act. Additionally, where it confers power, for instance, the use of forensic tools to harvest evidence, data retention, processing and inter-agency information sharing, it should also keep that power in check through necessary judicial oversight mechanisms. This is meant to protect national security and personal security which is right of the people to be secure. This form of security is a central component of the right to privacy. The protection of security is important to free societies, individual liberty, self-government, economic growth, and basic ideals of citizenship. It has a normative basis, first in articles 12 of the Universal Declaration of Human Rights and 17 of the International Covenant on Civil and Political Rights and Human Rights Committee General Comment 16, which provide that breaches of the right to privacy can only be justified when they are necessary to achieve a legitimate aim, prescribed by the law, and are proportionate to the aim pursued. It is not acceptable to use national security concerns as a blanket justification to excuse unwarranted privacy breaches; and secondly in article 19 of the Universal Declaration of Human Rights and of the International Covenant on Civil and Political Rights as read with the Human Rights Committee General Comment 34 to the Covenant, which specify the grounds on which speech can be restricted, regardless of frontiers and media. Cybercrime legislation should also sit within the broad national cyber security policy framework, in the case of Zimbabwe, within the Declaration of Rights in the Constitution, then national security framework provided for under the National ICT Policy, 2016; the draft Cyber Security Policy, and existing legislation such as the Interception of Communications Act (ICA) 2007, sections of the Criminal Law Codification and Reform Act, sections of Public Order and Security Act, sections of Access to Information and Protection of Privacy Act and the also within regional multilateral instruments such as the Africa Convention on Cybersecurity and Personal Data Protection (Malabo Protocol), although Zimbabwe hasn't adopted or ratified it

and the protocol is not yet in force. Ideally the bill should be accompanied by a detailed guidance on its application most importantly to ensure that individual rights as spelt out in national constitution and international law are secured. The Association for Progressive Communications (APC) and LARUE Framework is good starting point. APC developed the framework based on the work of Frank La Rue and on General Comment 34 on Article 19 of the ICCPR. The questions in the framework are intended to provide guidance in monitoring and reporting on internet-related human rights violations, specifically those related to freedom of expression. Further in the Appendix, we discuss cybersecurity concepts such as malware and digital forensics. A basic understanding of these terms can aid the law making and review process. The definitions are broader than those proffered in the draft Cybersecurity Policy (2015).

1. Core Definition of Cyber Crime.

'Definitions' of cybercrime mostly depend upon the purpose of using the term. A limited number of acts against the confidentiality, integrity and availability of computer data or systems represent the core of cybercrime. *See Appendix 1 for a further explanation of data confidentiality, integrity and availability*.

Other criminalised acts that may be included in cybercrime legislation

Beyond the core definition are other computer-related acts for personal or financial gain or harm, including forms of identity-related crime, and computer content-related acts (all of which fall within a wider meaning of the term 'cybercrime').

There are also 14 acts commonly included in notions of cybercrime which are: Illegal access to a computer system; illegal access, interception or acquisition of computer data; illegal data interference or system interference; production, distribution or possession of computer misuse tools; breach of privacy or data protection measures; computer-related fraud or forgery; computer-related identity offences; computer-related copyright and trademark offences; computer-related acts causing personal harm; computer-related acts involving racism or xenophobia; computer-related production, distribution or possession of child pornography; computer-related solicitation or 'grooming' of children; and computer-related acts in support of terrorism offences. This reflects a certain baseline consensus on culpable cybercrime conduct. Broadly the offences are also classified as; computer as a target, committed through the computer; content related offences and offence against the person.

Some countries have a few additional crimes mostly concerned with computer generated or disseminated content, including criminalization of obscene material (adult pornographic material), online gambling, and online illicit markets, such as in drugs and persons. While high-level consensus exists regarding broad areas of criminalization, detailed analysis of the provisions in source legislation reveals divergent approaches. Offences involving illegal access to computer systems and data differ with respect to the object of the offence (data, system, or information), and regarding the criminalization of 'mere' access or the requirement for further intent, such as to cause loss or damage.

The requisite intent for an offence also differs in approaches to criminalization of interference with computer systems or data. Most countries require the interference to be intentional, while others include reckless interference. For interference with computer data, the conduct constituting interference ranges from damaging or deleting, to altering, suppressing, inputting or transmitting data.

Criminalization of illegal interception differs by virtue of whether the offence is restricted to non-public data transmissions or not, and concerning whether the crime is restricted to interception 'by technical means'. Not all countries criminalize computer misuse tools. For those that do, differences arise regarding whether the offence covers possession, dissemination, or use of software (such as malware) and/or computer access codes (such as victim passwords). From the perspective of international cooperation, such differences may have an impact upon findings of dual-criminality between countries.

A number of content-related offences, particularly those concerning child pornography, show widespread criminalization. Differences arise however regarding the definition of 'child', limitations in relation to 'visual' material or exclusion of simulated material, and acts covered. Although the vast majority of countries, for instance, cover production and distribution of child pornography, criminalization of possession and access shows greater variation.

For computer-related copyright and trademark infringement, countries most usually reported the application of general criminal offences for acts committed wilfully and on a commercial scale.

The increasing use of social media and user-generated internet content has resulted in regulatory responses from governments, including the use of criminal law, and calls for respect for rights to freedom of expression.

Responding countries report varying boundaries to expression, including with respect to defamation, contempt, threats, incitement to hatred, insult to religious feelings, obscene material, and undermining the state. The socio-cultural element of some limitations is reflected not only in national law, but also in multilateral instruments. Some regional cybercrime instruments, for example, contain broad offences regarding the violation of public morals, pornographic material, and religious or family principles or values.

International human rights law acts both as a sword and a shield, requiring criminalization of (limited) extreme forms of expression, while protecting other forms.[1]

Some prohibitions on freedom of expression, including incitement to genocide, hatred constituting incitement to discrimination, hostility or violence, incitement to terrorism, and propaganda for war, are therefore required for States that are party to relevant international human rights instruments.

For others, the 'margin of appreciation' allows leeway to countries in determining the boundaries of acceptable expression in line with their own cultures and legal traditions. Nonetheless, international human rights law will intervene at a certain point.[2]

Penal laws on defamation, disrespect for authority, and insult, for example, that apply to online expressions will face a high threshold of demonstrating that the measures are proportionate, appropriate, and the least intrusive possible.

---

[1] Article 19 of the Universal Declaration of Human Rights and of the International Covenant on Civil and Political Rights as read with the Human Rights Committee General Comment 34 to the Covenant, which specify the grounds on which speech can be restricted, regardless of frontiers and media.

[2] The Association for Progressive Communications (APC) and LARUE Framework is good starting point. APC developed the framework based on the work of Frank La Rue and on General Comment 34 on Article 19 of the ICCPR. The questions in the framework are intended to provide guidance in monitoring and reporting on internet-related human rights violations, specifically those related to freedom of expression. Further work is needed, and is underway, to develop more comprehensive guidance

Where content is illegal in one country, but legal to produce and disseminate in another, States will need to focus criminal justice responses on persons accessing content within the national jurisdiction, rather than on content produced outside of the country.

2. Law enforcement and investigations

Over 90 per cent of responding countries report that cybercrime acts most frequently come to the attention of law enforcement authorities through reports by individual or corporate victims. Responding countries estimate that the proportion of actual cybercrime victimization reported to the police ranges upwards from 1 per cent. Zimbabwe has experienced some of these crimes based on Reserve Bank of Zimbabwe reports (2015).[3]

One global private sector survey suggests that 80 per cent of individual victims of core cybercrime do not report the crime to the police. Underreporting derives from a lack of awareness of victimization and of reporting mechanisms, victim shame and embarrassment, and perceived reputation risks for corporations.

Authorities in all regions of the world highlighted initiatives for increasing reporting, including online and hotline reporting systems, public awareness campaigns, private sector liaison, and enhanced police outreach and information sharing.

An incident-driven response to cybercrime must, however, be accompanied by medium and long-term tactical investigations that focus on crime markets and criminal scheme architects. Law enforcement authorities in developed countries are engaged in this area, including through undercover units targeting offenders on social networking sites, chat rooms, and instant messaging and peer to peer (P2P) services.

Challenges in the investigation of cybercrime arise from criminal innovations by offenders, difficulties in accessing electronic evidence, and from internal resource, capacity and logistical limitations. Suspects frequently use anonymization and obfuscation technologies, and new techniques quickly make their way to a broad criminal audience through online crime markets.

Law enforcement in cybercrime investigations require an amalgamation of traditional and new policing techniques. While some investigative actions can be achieved with traditional powers, many procedural provisions do not translate well from a spatial, object-oriented approach to one involving electronic data storage and real-time data flows.

A cybercrime law should ideally specify cybercrime investigative measures, ranging from generic search and seizure to specialized powers, such as preservation of computer data, and data verification and authenticity.

National approaches to investigative measures for cybercrime generally include:

- Search
- Seizure
- Order for subscriber data
- Order for traffic data
- Order for content data
- Real time traffic data
- Real time content data
- Expedited preservation

[3] http://www.rbz.co.zw/assets/cybercrime-globally-and-in-zimbabwe.pdf

- Remote forensics
- Trans-border access

Countries most often reported the existence of general (non-cyber-specific) powers across all investigative measures. A number of countries also reported cyber-specific legislation, notably for ensuring expedited preservation of computer data and obtaining stored subscriber data.

Many countries reported a lack of legal power for advanced measures, such as remote computer forensics. The law should therefore specifically authorise the use of forensic devices, in order for such usage to be lawful. The use of remote computer forensic requires judicial oversight as it might be susceptible to abuse. This entails, for instance, installing software on computers, computer servers or facilities that relay inform to the investigating authorities with or without the knowledge of data subject. When such data is collected safeguards should be put in place, this might mean attending to Electronic Evidence Rules or Act which might speak to this or revisiting the Criminal Procedure and Evidence Act.

While traditional procedural powers can be extended to cyber situations, in many cases such an approach can also lead to legal uncertainties and challenges to the lawfulness of evidence gathering, and thus the admissibility of evidence. Overall, national approaches to cybercrime investigative powers show less core commonality than for criminalization of many cybercrime acts.

Irrespective of the legal form of investigative powers, all responding authorities use search and seizure for the physical appropriation of computer equipment and the capture of computer data. The majority of countries also use orders for obtaining stored computer data from internet service providers.

Outside of Europe, however, around one third of countries report challenges in compelling third parties in an investigation to provide information.

Around three-quarters of countries use specialized investigative measures, such as real-time collection of data, or expedited preservation of data. Use of investigative measures typically requires a minimum of initial evidence or a report of a cybercrime act.

More intrusive measures, such as those involving real-time collection of data or accessing of data content, often require higher thresholds, such as evidence of a serious act, or demonstration of probable cause or reasonable grounds.[4]

The interplay between law enforcement and internet service providers is particularly complex. Service providers hold subscriber information, billing invoices, some connection logs, location information (such as cell tower data for mobile providers), communication content, all of which can represent critical electronic evidence of an offence.[5]

National legal obligations and private sector data retention and disclosure policies vary widely by country, industry and type of data. Countries most often reported using court orders to obtain evidence from service providers.

[4] The Zimbabwe Interception of Communications Act (ICA) 2007 should be harmonised with the cybercrime bill.

[5] Note that the use of Sting Rays (IMSI Catchers) has been criticised by scholars on the ground that as these are military technologies, they are unsuitable in civilian spaces.

In some cases, however, law enforcement may be able to obtain stored subscriber data, traffic data, and even content data, directly.[6] In this respect, private sector organizations often reported both a primary policy of requiring due legal process for data disclosure, but also voluntary compliance with direct law enforcement requests under some circumstances. Zimbabwe does not have a data protection law in place beyond the limited provisions of the Access to Information and Protection of Privacy Act (AIPPA); therefore standards of protection of data are missing such as lawful and fair collection; use for specific purpose for which it was originally collected; not excessive to purpose; accurate; secure and destroyed after purpose use.

Informal relationships between law enforcement and service providers, the existence of which was reported in more than half of all responding countries, assist the process of information exchange and trust-building. Responses indicated that there is a need to balance privacy and due process, with disclosure of evidence in a timely manner, in order to ensure that the private sector does not become a 'choke-point' for investigations.

Cybercrime investigations invariably involve considerations of privacy under international human rights law. Human rights standards specify that laws must be sufficiently clear to give an adequate indication of the circumstances in which authorities are empowered to use an investigative measure, and that adequate and effective guarantees must exist against abuse.[7] Countries reported the protection of privacy rights in national law, as well as a range of limits and safeguards on investigations. When investigations are transnational, divergences in levels of protection, however, give rise to unpredictability regarding foreign law enforcement access to data, and potential jurisdictional gaps in privacy protection regimes.

Over 90 per cent of the countries that participated in the research have begun to put in place specialized structures for the investigation of cybercrime and crimes involving electronic evidence.[8]

In developing countries, however, these are not well resourced and suffer from a capacity shortage. Countries with lower levels of development have significantly fewer specialized police, with around 0.2 per 100,000 national internet users. The rate is two to five times higher in more developed countries. Seventy per cent of specialized law enforcement officers in less developed countries were reported to lack computer skills and equipment, and only half receive training more than once a year.

More than half of responding countries in Africa, and one-third of countries in the Americas report that law enforcement resources for investigating cybercrime were insufficient. Globally, it is likely that the picture is worse. The study received responses, for example, from only 20 per cent of the world's 50 least developed countries.

All responding countries in Africa, and over 80 per cent of countries in the Americas and Asia and Oceania reported requiring technical assistance. The most commonly cited area for technical assistance required was general cybercrime investigative techniques. Of those

[6] There is need for transparency in the use of data mining techniques, especially dual use of technologies such as Deep Packet and Deep Content Inspection (DPI and DCI) respectively. The Human Rights Council is encouraging companies to follow the rule of law. When a state says to take down this post or block this website, or give us this or that data without proper oversight mechanisms, such as a warrant, the UN hope that they're pushing back and behaving according to human rights norms.

[7] International Covenant on Civil and Political Rights Article 17; regional conventions including Article 10 of the African Charter. the Human Rights Committee General Comment 16 on the interpretation of article 17 of the ICCPR

[8] The African Convention on Cybersecurity specifies this too.

countries requiring assistance, 60 per cent indicated that this was needed by law enforcement agencies.

3. Electronic evidence and criminal justice[9]

Evidence is the means by which facts relevant to the guilt or innocence of an individual at trial are established. Electronic evidence is all such material that exists in electronic, or digital, form.

It can be stored or transient. It can exist in the form of computer files, transmissions, logs, metadata, or network data. Digital forensics is concerned with recovering – often volatile and easily contaminated – information that may have evidential value. Forensics techniques include the creation of 'bit-for-bit' copies of stored and deleted information, 'writeblocking' in order to ensure that the original information is not changed, and cryptographic file 'hashes', or digital signatures, that can demonstrate changes in information.

Almost all countries reported some digital forensics capacity. Many responding countries, across all regions, however, note insufficient numbers of forensic examiners, differences between capacity at federal and state level, lack of forensics tools, and backlogs due to overwhelming quantities of data for analysis. One half of countries report that suspects make use of encryption, rendering access to this type of evidence difficult and time-consuming without the decryption key.

In most countries, the task of analyzing electronic evidence lies with law enforcement authorities. Prosecutors, however, must view and understand electronic evidence in order to build a case at trial.

All countries in Africa and one-third of countries in other regions reported insufficient resources for prosecutors to do so. Prosecution computer skills are typically lower than those of investigators.

Globally, around 65 per cent of responding countries report some form of prosecutorial cybercrime specialization. Just 10 per cent of countries report specialized judicial services. The vast majority of cybercrime cases are handled by non-specialized judges, who, in 40 per cent of responding countries, do not receive any form of cybercrime-related training. Judicial training on cybercrime law, evidence collection, and basic and advanced computer knowledge represents a particular priority.

Over 60 per cent of responding countries do not make a legal distinction between electronic evidence and physical evidence. While approaches vary, many countries consider this good practice, as it ensures fair admissibility alongside all other types of evidence.

A number of countries outside of Europe do not admit electronic evidence at all, making the prosecution of cybercrime, and any other crime evidenced by electronic information, unfeasible. While countries do not, in general, have separate evidentiary rules for electronic evidence, a number of countries referred to principles such as: the best evidence rule, the relevance of evidence, the hearsay rule, authenticity, and integrity, all of which may have particular application to electronic evidence.

Many countries highlighted challenges of attribution of acts to a particular individual, and commented that this was often dependent upon circumstantial evidence.

---

[9] **See-** Legal Opinion on Intercept Communication - University of Oxford

The challenges facing both law enforcement investigators and prosecutors mean that 'brought to justice' rates are low for cybercrime offenders. Suspects identified per police recorded offence are comparable for child pornography offences to other sex offences. However, suspects per recorded offence for acts such as illegal access and computer-related fraud or forgery are only around 25 per 100 offences. Very few countries were able to provide data on persons prosecuted or convicted. Calculations for cybercrime offences in one country, however, show that the ratio of persons convicted to recorded offences, is significantly lower than for other 'conventional' crimes.

4. International cooperation

Countries that participated in the study report that between 30 and 70 per cent of cybercrime acts involve a transnational dimension, engaging issues of transnational investigations, sovereignty, jurisdiction, extraterritorial evidence, and a requirement for international cooperation. In respect of jurisdiction, three issues arise in respect of computer and cyber-crimes; does the state have the legislative power to regulate the relevant conduct which is usually prescriptive jurisdiction; do the courts have the powers to hear that particular issue which is adjudicative jurisdiction and lastly the state have the jurisdiction to enforce the law which is enforcement jurisdiction. A cybercrime framework has to take all this into account.

A transnational dimension to a cybercrime offence arises where an element or substantial effect of the offence is in another territory, or where part of the modus operandi of the offence is in another territory.

International law provides for a number of bases of jurisdiction over such acts, including forms of territory-based jurisdiction and nationality based jurisdiction. Some of these bases are also found in multilateral cybercrime instruments.

While all countries in Europe consider that national laws provide a sufficient framework for the criminalization and prosecution of extraterritorial cybercrime acts, around one-third to over one-half of countries in other regions of the world report insufficient frameworks.

In many countries, provisions reflect the idea that the 'whole' offence need not take place within the country in order to assert territorial jurisdiction. Territorial linkages can be made with reference to elements or effects of the act, or the location of computer systems or data utilized for the offence. Where they arise, jurisdictional conflicts are typically resolved through formal and informal consultations between countries. Country responses do not reveal, at present, any need for additional forms of jurisdiction over a putative 'cyberspace' dimension. Rather, forms of territoriality-based and nationality-based jurisdiction are almost always able to ensure a sufficient connection between cybercrime acts and at least one State.

Forms of international cooperation include extradition, mutual legal assistance, mutual recognition of foreign judgments, and informal police to-police cooperation.

Due to the volatile nature of electronic evidence, international cooperation in criminal matters in the area of cybercrime requires timely responses and the ability to request specialized investigative actions, such as preservation of computer data.

Use of traditional forms of cooperation predominates for obtaining extra-territorial evidence in cybercrime cases, with over 70 per cent of countries reporting using formal mutual legal assistance requests for this purpose. Within such formal cooperation, almost 60 per cent of requests use bilateral instruments as the legal basis. Multilateral instruments are used in 20 per cent of cases.

Response times for formal mechanisms were reported to be of the order of months, for both extradition and mutual legal assistance requests, a timescale which presents challenges to the collection of volatile electronic evidence.

Sixty per cent of countries in Africa, the Americas and Europe, and 20 per cent in Asia and Oceania, report channels for urgent requests. However, the impact of these on response times is unclear. Modes of informal cooperation are possible for around two-thirds of reporting countries, although few countries have a policy for the use of such mechanisms.

Initiatives for informal cooperation and for facilitating formal cooperation, such as 24/7 networks, offer important potential for faster response times. They are, however, under-utilized, handling around three per cent of the total number of cybercrime cases encountered by law enforcement for the group of reporting countries.

Formal and informal modes of cooperation are designed to manage the process of State consent for the conduct of foreign law enforcement investigations that affect a State's sovereignty. Increasingly, however, investigators, knowingly or unknowingly, access extraterritorial data during evidence gathering, without the consent of the State where the data is physically situated. This situation arises, in particular, due to cloud computing technologies which involve data storage at multiple data centres in different geographic locations.

Data 'location', whilst technically knowable, is becoming increasingly artificial, to the extent that even traditional mutual legal assistance requests will often be addressed to the country that is the seat of the service provider, rather than the country where the data centre is physically located. Direct foreign law enforcement access to extraterritorial data could occur when investigators make use of an existing live connection from a suspect's device, or where investigators use lawfully obtained data access credentials.

Law enforcement investigators may, on occasion, obtain data from extra-territorial service providers through an informal direct request, although service providers usually require due legal process. Relevant existing provisions on 'trans-border' access found in the Council of Europe Cybercrime Convention and the League of Arab States Convention on Information Technology Offences do not adequately cover such situations, due to a focus on the 'consent' of the person having lawful authority to disclose the data, and presumed knowledge of the location of the data at the time of access or receipt.

The current international cooperation picture risks the emergence of country clusters that have the necessary powers and procedures to cooperate amongst themselves, but are restricted, for all other countries, to 'traditional' modes of international cooperation that take no account of the specificities of electronic evidence and the global nature of cybercrime. This is particularly the case for cooperation in investigative actions.

A lack of common approach, including within current multilateral cybercrime instruments, means that requests for actions, such as expedited preservation of data outside of those countries with international obligations to ensure such a facility and to make it available upon request, may not be easily fulfilled.

The inclusion of this power in the African Union Cybersecurity Convention may go some way towards closing this lacuna. Globally, divergences in the scope of cooperation provisions in multilateral and bilateral instruments, a lack of response time obligation, a lack of agreement on permissible direct access to extraterritorial data, multiple informal law enforcement networks, and variance in cooperation safeguards, represent significant

challenges to effective international cooperation regarding electronic evidence in criminal matters.

5. Cybercrime prevention

Crime prevention comprises strategies and measures that seek to reduce the risk of crimes occurring, and mitigate potential harmful effects on individuals and society. Almost 40 per cent of responding countries report the existence of national law or policy on cybercrime prevention. Initiatives are under preparation in a further 20 per cent of countries. Countries highlight that good practices on cybercrime prevention include the promulgation of legislation, effective leadership, development of criminal justice and law enforcement capacity, education and awareness, the development of a strong knowledge base, and cooperation across government, communities, the private sector and internationally.

More than one half of countries report the existence of cybercrime strategies. In many cases, cybercrime strategies are closely integrated in cybersecurity strategies. Around 70 per cent of all countries reported national strategies included components on awareness raising, international cooperation, and law enforcement capacity. For the purposes of coordination, law enforcement and prosecution agencies are most frequently reported as lead cybercrime institutions.

Surveys, including in developing countries, demonstrate that most individual internet users now take basic security precautions. The continued importance of public awareness raising campaigns, including those covering emerging threats, and those targeted at specific audiences, such as children, was highlighted by responding Governments, private sector entities, and academic institutions.

User education is most effective when combined with systems that help users to achieve their goals in a secure manner. If user cost is higher than direct user benefit, individuals have little incentive to follow security measures. Private sector entities also report that user and employee awareness must be integrated into a holistic approach to security.

Foundational principles and good practice referred to include accountability for acting on awareness, risk management policies and practices, board-level leadership, and staff training. Two-thirds of private sector respondents had conducted a cybercrime risk assessment, and most reported use of cybersecurity technology such as firewalls, digital evidence preservation, content identification, intrusion detection, and system supervision and monitoring. Concern was expressed, however, that small and medium-sized companies either do not take sufficient steps to protect systems, or incorrectly perceive that they will not be a target.

Regulatory frameworks have an important role to play in cybercrime prevention, both with respect to the private sector in general and service providers in particular. Nearly half of countries have passed data protection laws, which specify requirements for the protection and use of personal data.

Some of these regimes include specific requirements for internet service providers and other electronic communications providers. While data protection laws require personal data to be deleted when no longer required, some countries have made exceptions for the purposes of criminal investigations, requiring internet service providers to store specific types of data for a period of time. Many developed countries also have rules requiring organizations to notify individuals and regulators of data breaches. Internet service providers typically have limited liability as ‘mere conduits’ of data. Modification of transmitted content increases liability, as

does actual or constructive knowledge of an illegal activity. Expeditious action after notification, on the other hand, reduces liability. While technical possibilities exist for filtering of internet content by service providers, restrictions on internet access are subject to foreseeability and proportionality requirements under international human rights law protecting rights to seek, receive and impart information.

Public-private partnerships are central to cybercrime prevention. Over half of all countries report the existence of partnerships. These are created in equal numbers by informal agreement and by legal basis. Private sector entities are most often involved in partnerships, followed by academic institutions, and international and regional organizations.

Partnerships are mostly used for facilitating the exchange of information on threats and trends, but also for prevention activities, and action in specific cases. Within the context of some public-private partnerships, private sector entities have taken proactive approaches to investigating and taking legal action against cybercrime operations. Such actions complement those of law enforcement and can help mitigate damage to victims.

Academic institutions play a variety of roles in preventing cybercrime, including through delivery of education and training to professionals, law and policy development, and work on technical standards and solution development. Universities house and facilitate cybercrime experts, some computer emergency response teams (CERTs), and specialized research centres.

Structure of the Cyber Crime Bill

This structure is informed by the outline above but is not intended to be prescriptive neither is it exhaustive

Part I of the bill should cover the preliminaries, including definitions. Definitions for cybercrimes laws are critical and very much fluid as new terms are emerging or evolving. This section should take into account the other technology or electronic related laws in place and their definitions for instance the Postal and Telecommunications Act might have a definition of a computer system or device or electronic network.

Part II usually contains the provisions of the various offences, offences against the computer, through the computer, against the person and content related offences. This section also needs to take account of the existing laws and those provisions that might be affected such as in the Criminal Law (Code).

Part III can deal with aspects relating to evidence admission in court, collection, storage and authenticity. This section has to be consistent with provisions that might be in other laws such as the Data Protection law among others. In addition, some jurisdictions have developed separate Electronic Evidence Acts (Botswana, Tanzania, and Uganda). This can also be part of jurisdiction related issues, including extradition, mutual assistance among others. Bearing in mind those issues of criminal mutual assistance might also be dealt with by other laws and specific

Part IV can deal with aspects of the computer emergency response facilities or team. This would entail laying out its mandate, composition, responsibilities, duties, powers and relations with other cyber security stakeholders, including private sector, government agencies etc.

Part V can deal with issues relating to third party service providers who, for instance, might have to comply with forensic tools installation on their systems. This section has to be consistent with section of ICA. This section might also cover aspects to do with intermediary liability etc.

Part VI can have general provisions, consequential amendments etc.