Project Cybercrime@Octopus

Strasbourg, France
Version 9 December 2014
(Provisional)

Cybercrime Model Laws

Discussion paper prepared for the
Cybercrime Convention Committee (T-CY)

Zahid Jamil
Consultant
Jamil & Jamil
Barrister-at law
Pakistan

www.coe.int/cybercrime

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Contents

Contact

Alexander Seger
Head of Cybercrime Programme Office (C-PROC)
Directorate General of Human Rights and Rule of Law
Council of Europe, Strasbourg, France
Tel +33-3-9021-4506
Fax +33-3-9021-5650
Email: alexander.seger@coe.int

Disclaimer

This technical report does not necessarily represent official positions of the Council of Europe, of Parties to treaties referred to or of the donors to capacity building projects.

1 Introduction

This paper aims to discuss the role and purpose of cybercrime model laws in the context of the only existing and effective global treaty on cybercrime, the Budapest Convention (the "Convention"). The paper will layout the general landscape with respect to those texts currently perceived as cybercrime model laws. A brief summary of their content will be followed by a detailed analysis that will focus on their strengths and weaknesses as well as their consistency and compatibility with the Budapest Convention. This will be followed by identifying known instances where these model laws have been utilized and/or implemented. Finally the paper will attempt to draw some conclusions and provide possible recommendations.

1.1 The Convention and model legislation

The implementation of holistic, compatible and convergent cybercrime legislation on a global basis is an essential, if not the fundamental, component of any global response to effectively combatting cybercrime. In addition to establishing an international legal framework for cooperation, the Convention requires member states to implement just such holistic, compatible and convergent legislation. This is effected through principles enumerated in the various Articles of the Convention. Being a treaty instrument the Convention does not provide specific legislative language for implementation of the principles outlined by its provisions, although the language of the Convention has been used by a number of countries to draft domestic legislation. It thus, leaves the precise language for implementation of the principles enshrined in treaty obligations to the discretion of each sovereign member state. Thereby respecting the sovereignty of each member state as well as recognizing that each state varies in terms of its legal system and legislative process.

Legislation and the legislative processes for most nations remain even in the 21st Century a slow and painful process. This is a challenge to the implementation of the necessary enabling legal environment required for effective international cooperation in investigation and prosecution of cybercrime, particularly given the global and exponential growth of cybercrime. Nowhere is the challenge more apparent and greatly experienced than by developing countries or those countries that lack the capacity to draft cybercrime and electronic evidence legislation, both of which require specialized skill and expertise. Given the dearth of such available skill and resource many countries look outwards for tools and resources accessible over the internet and towards international organizations for this capacity. The type of assistance (especially developing countries) seek in this respect is an assistance in actually drafting their legislation whilst ensuring the legislation satisfies both local law requirements as well as compatibility with international best practice.

In the case of current or future parties to the Convention, the treaty is the definitive benchmark of international best practice. The Convention has also been the benchmark for countries who are not members or have not ratified/requested accession. Furthermore, the Convention has been largely followed by most attempts to draft model legislation[1] on cybercrime and its principles largely emulated in other efforts to draft an international instrument[2] on cybercrime.

[1] Commonwealth Model Law, ITU Model Laws

[2] African Union Convention on Cybersecurity, COMJIB (Conference of Ministers of Justice of Ibero-American Countries) etc..

Currently, there are various attempts to develop model laws. Some models bear approval of States in some form[3], whilst others that lack any form of State approval with little specialized expertise and are, at times, rather poor in their attempts to fashion so-called model legislative texts[4].

In fact, the status of these so-called model laws is rather confusing. One would assume that model laws developed or promoted by international organisations are negotiated through formal procedures and inter-governmental processes.[5] This matters both in terms of agreement on substance but also in terms of inter-governmental acceptance and credibility. With the exception of the Commonwealth Model Law, no other Model Laws appear to have been the product of any such inter-governmental process. In fact, "Model Laws" are abound giving the perception of formal approval when in fact no such approval appears to have been provided by member states of these inter-governmental bodies.

1.2 Purpose of a Model Law on Cybercrime

A Model Law should attempt to bridge the best practice principles of substantive offences, powers, and mutual legal assistance, such as those enunciated by the Convention, with specific examples of language that elaborate the various elements that need to be included in a law when implementing these principles. For instance, when drafting legislation enabling search and seizure in terms of Article 19 of the Convention, simply copying the language of the Convention or somewhat elaborating upon the powers might not be sufficient to meet the standard expected under the Convention. Additionally, specific principles of Article 15 which require establishment of countervailing conditions and safeguards to balance the special and intrusive powers also need to be included in any legislative provision for search and seizure. Article 15 simply provides guidance at a high level, listing principles applicable to each special power or procedure mandated by the Convention such as respect for human rights, the principle of proportionality, judicial or other independent supervision, grounds justifying application, establishment of limits to the scope and duration of each power or procedure as well as considering the impact upon the rights, responsibilities and legitimate interests of third parties. These very broad principles can be interpreted in a myriad of ways and thus can be the subject of great variation in the levels of quality in terms of implementation. For instance, the Commonwealth Model Law drafters thought that the principle of "grounds justifying application" would simply require adding the words "reasonable grounds", without elaborating what these words would mean in the context of the different powers mandated by the Convention. One has to turn to legislation from jurisdictions such as the US, UK and Singapore for instances of grounds.

Given this, States that might read Article 19 in isolation may not realize the need to add principles of Article 15 when implementing Article 19 into their legislation. Those States that do realize this may simply add minimal language (such as the Commonwealth Model Law and other models have done) rather than the very detailed provisions necessary to provide implementation of both Article 19 and Article 15 when drafting legislation for search and seizure of computer

[3] Law Ministers approval of the Commonwealth Model Law and its recognition by the Heads of Government Meeting

[4] ITU Model Laws, World Bank's EGRIP Model Law

[5] See, for example, the procedure involved in the development and adoption of UNCITRAL model laws: http://www.uncitral.org/pdf/english/texts/procurem/ml-procurement-2011/2011-Model-Law-on-Public-Procurement-e.pdf

data. Thus, simply relying upon the language of the existing model laws would not equal effective implementation of the Convention.

Poorly drafted model laws that diverge from international best practice can have a negative effect upon the readiness of nations to combat cybercrime and cooperate internationally. States, in particular those that possibly lack the necessary skills to draft cybercrime and electronic evidence laws, which rely upon such divergent or poorly drafted models laws are likely to incorporate these into their legislation. They may do so under the mistaken belief that since these models appear to be supported by international organizations, they represent a certain level of quality and international best practice. Having gone through the arduous process of drafting and passing legislation they may come to realize, possibly when they seek to cooperate across borders with law enforcement or seek their cooperation that they face challenges due to their having followed such poor and divergent model laws. For instance, most if not all model laws currently available only deal with two of the three segments covered by the Convention. They attempt to cover substantive offences and powers and procedures but fail either adequately or altogether to cover international cooperation. Only the Commonwealth Model law makes mention of international cooperation and explains that the next iteration of the Commonwealth Harare Scheme would (and now does) deal with this aspect. ITU's ICB4PAC makes a general mention of international cooperation in one provision, but does not provide the legislative language necessary for international cooperation or mutual legal assistance either as provided in the Convention or as suggested by the Commonwealth's Harare Scheme. It has been a challenge in some Nations to explain that, despite several model laws not addressing international cooperation, these provisions are essential to combat what is a global threat. At times, stakeholders have even argued in some nations that it was their reading of Chapter 3 of the Convention related to international cooperation, that these provisions were neither really relevant nor related to Cybercrime and were in fact provisions a State could simply ignore and still holistically address the issue of cybercrime from a legislative perspective. Hours of discussion and explanation were required to explain the essential nature of Chapter 3 of the Convention.

All models have excluded provisions related to intellectual property/digital copyright (Article 10) without any explanation or comment (such as it should be dealt with in copyright legislation). Although Article 10 does not require countries to ratify or accede to the various Copyright treaties listed in the Article, the absence of the offence without any mention or commentary, in what should be a representation of best practice, tends to give the impression that criminalizing of digital copyright is not necessary to combat cybercrime. Most law enforcement officials and prosecutors will support the fact that one of the most effective means of combatting cybercriminals is the use of criminal offences with respect to digital copyright offences. For instance, they tend to be highly useful if not essential in combatting phishing and e-fraud and e-forgery. Yet other Models have chosen to exclude e-fraud and e-forgery without any explanation. Other models criminalize conduct which is not usually a crime but a regulated activity requiring an entirely separate and self-contained legislation, for instance SPAM. Such models criminalize all forms of SPAM and dismiss the issue as an offence in a few lines of legislative language when the issue is far more complicated, merits greater attention and requires holistic legislation. Thus, poorly drafted and divergent model laws can cause countries to enact cybercrime legislation with gaping lacunas whilst at the same time criminalizing and labelling conduct as cybercrime which other countries (especially many members to the Convention) from whom they may seek cooperation would never view as cybercrime. Such States might incorrectly perceive and thus, frame these as instances of the failure of members of the Convention in cooperating to combat conduct which in their minds appear to be internationally accepted forms of cybercrime recognized by such model laws. At times, when such poor and divergent efforts to produce model laws have been funded by or bear the flag of international organizations[6] (for instance the European Union[7]) it becomes a challenge to advocate against the poor practices disseminated by these model laws. What tends not to be clear is the fact that such models are simply funded by the executive arms of international organizations and are products of consultants which do not necessarily have the sanction of the international organization's general body or approval of member States. Needless to say, this tends to create a challenge both in terms of adoption of the Convention by such States and is a barrier to the implementation of holistic, compatible, convergent and effective cybercrime legislation on a global basis.

As mentioned above, this is precisely why any work with respect to model laws should be taken very seriously. It should be ensured that approval and sanction by international organizations or their executive bodies or secretariats should not extend to documents purporting to bear the label of "Model" "Legislation" "Texts" or similar without a thorough examination of their quality and their having gone through the important process of inter-governmental negotiations and approval.

2 Current Landscape

Presently there are five salient texts that appear to have found prominence amongst many States, particularly in the developing world.

2.1 The Commonwealth Model Law

Requisitioned by the Commonwealth Law Ministers, an expert group on Computer Crime and Related Criminal Law was established and in 2002 prepared a revised Model Law on Computer and Computer Related Crime [***"Commonwealth Model Law"***] which was based upon the Council of Europe Convention on Cybercrime.[8] This draft has received much recognition being a reasonable first effort at a model law based upon the Convention. It has imperfections which are discussed below. Though not widely adopted by many States, the fact that much of its framework and provisions have found their way into the ITU model laws have consequently led to many of its provisions being implemented (though clouded by many poor edits by the ITU) into legislation by nations in the Caribbean, Africa and the Pacific. Until very recently, the Model Law was largely overlooked by the Commonwealth. Even recent calls by the Commonwealth Heads of Government and the Commonwealth Cybercrime initiative appear not to place the Model law front and center of a strategy in connection with Cybercrime. At present it appears to have been removed from the Commonwealth Secretariat's website[9] and is unavailable through a cursory Google search. It has thus regrettably, been of limited relevance in terms of impact upon Commonwealth countries or even generally.

It is important to note that this is the only Model Law analyzed as part of this paper that bears any resemblance to an official inter-governmental process for negotiation and approval.

[6] ITU, Commonwealth, World Bank

[7] HIPCAR, ICB4PAC, HIPSSA

[8] LMM(02)17 – Report to Law Ministers @ page 1

[9] http://thecommonwealth.org/shared_asp_files/uploadedfiles/%7bDA109CD2-5204-4FAB-AA77-86970A639B05%7d_Computer%20Crime.pdf – "Page not found
The requested page "/shared_asp_files/uploadedfiles/%7bDA109CD2-5204-4FAB-AA77-86970A639B05%7d_Computer%20Crime.pdf" could not be found."

2.2 The Three ITU Model Laws

Three are the product of an ITU run @CP-ICT Programme that was funded by the 9th European Development Fund (EDF) of the European Union and co-financed by the ITU focusing on three regions: Africa, the Caribbean and the Pacific islands (ACP)[10] and is described as a global ITU-EC-ACP project[11] The three arise from the following three projects:

- Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean - **Cybercrime/e-crime: Model** Policy Guidelines & **Legislative Texts** [***"HIPCAR"***]
- ITU-EC project on Capacity Building and ICT policies, Regulations and Legislative Frameworks" for Pacific Islands Countries - **Pacific Island Regional Model Cybercrime Legislation** [***"ICB4PAC"***]
- Harmonization of ICT Policies in Sub-Saharan Africa - Computer Crime and Cybercrime: Southern African Development Community (SADC) Model Law [*"HIPSSA"*]

Interestingly, even across the three regions and projects there appears to be a lack of harmonization in terms of their subject matter or title and range between e-crime, cybercrime, computer crime. From information so far available it appears that these models have had an impact in terms of the numbers of countries (largely in the Caribbean, Africa and Pacific Islands) that seem to have utilized these models when drafting their cybercrime legislation. The Models largely appear to have been prepared through input from participants at workshops rather than representatives or experts with an official mandate from State parties and have not received any official assent from the general body of the ITU. They appear to be sourced from a draft prepared by ITU consultants who attempted to use the general framework and much of the language from the Commonwealth Model Law but with substantial modifications, additions and deviations from international best practice. In particular, introducing provisions that would raise human rights and freedom of speech concerns, enable content control, and regressive powers without safeguards which substantially impact industry, online providers and users in a manner inconsistent with OECD work in this area.

It is noteworthy that though the models bear the flags, emblems and logos and make mention of project funded by the ITU, EU and regional bodies they were not part of any official inter-governmental negotiations and approvals process. Their status and credibility as "Model Laws", officially supported by the general bodies of the inter-governmental organizations named in their products, are at best dubious.

2.3 The World Bank-OECS Model Law

This is a regional model law initiative funded by the **World Bank** for the Organization of Eastern Caribbean States **(OECS)** under the Electronic Government for Regional Integration Project with several model legislations including the **Model Electronic Crimes Bill** [***"EGRIP"***][12]. It appears to have been the work of Hellerstein & Associates as Consultants. Their lead consultant has "worked with several West African, Caribbean, Western CIS, Latin America, and East Asian Countries on developing new ICT, e-Commerce, Cyber and computer crime, and e-Government laws" and "In 2011, ….. provided advisory services to the OECS, a regional organization for Eastern Caribbean states, on ways of reforming their e-commerce and e-transaction laws,

[10] http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/Pages/default.aspx

[11] HIPCAR Cybercrime/e-Crimes: Model Policy Guidelines & Legislative Texts Acknowledgements @ page iii

[12] http://www.oecs.org/publications/e-government-for-regional-integration-project/oecs-harmonized-e-government-legislation - E-Crime Bill is marked as a "Popular" download

designing training programs on cyber crime, e-commerce and other related ICT laws."[13] This Model Law does not appear to follow any recognizable international best practice model and in terms of structure, provisions and language is the most unique of the five model laws. Although discussed further below this model appears to be the most challenging in terms of harmonization, compatibility and consistency with international best practice. It also creates and establishes offences and criminalizes social conduct on the internet which would not be viewed by developed countries as criminal, and only contains one provision which would be recognizable by way of cybercrime in the context of the Convention or the other four model laws. It appears to pose the greatest challenge in terms of the quality of legal and technical knowledge and skill. There is very little available by way of information about the consultative process but it appears from participants this model was also prepared through input from participants at workshops rather than representatives or experts with an official mandate from State parties and it is unclear if it has the assent of State parties to the World Bank or the World Bank at an institutional level.

It is important to point out that this Model Law appears to be the outcome of workshops and consultations with participants and not a document negotiated as part of any official inter-governmental process.

3 The Model Laws

Below is an analysis in the form of summaries for each Model Law which includes either separate or combined analysis of the strengths and weaknesses of each model law and instances of its implementation and impact with respect to national legislation.

For each Model we have attempted to develop a scoring process which is based upon our analysis of the adequacy of a purported text as a model cybercrime legislation. A set of criteria based upon international best practice in part based upon the Convention (since the Convention cannot and does not provide detailed legislative language) has been created which is available in the scoring tables annexed under section 5 of this paper. Methodology followed for instance includes marking nil where a criteria (possibly an Article of the Convention or other metric) is absent and scoring consistency with international best practice between 1 to 10 (10 being the highest). In case of language that detracts from international best practice or negates its principles or is unsafe in some respect, negative scores are allotted. This method is being attempted for the first time in this area and should be the subject of further discussion for improvement with the aim eventually of possible dissemination, to assist in transparency with respect to quality and consistency with international best practice of these texts, particularly for the benefit of developing countries and their stakeholders.

3.1 ITU Models Legislative texts

The Model Legislations of the global ITU-EC-ACP project[14] implemented by the ITU and funded by the EU[15] are widely circulated and acknowledged by several States both in the projects target regions and beyond as representing best practice. With these Model Laws, countries in the Caribbean, Pacific and Sub-Saharan Africa are drafting and implementing legislation that diverge from the norm in terms of definitions, cybercrime offences and powers. Regulatory powers

[13] http://www.jhellerstein.com/about.html

[14] HIPCAR Cybercrime/e-Crimes: Model Policy Guidelines & Legislative Texts Acknowledgements @ page iii

[15] http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/Pages/default.aspx

introduced in the Models give governments and public authorities sweeping, overly broad and intrusive powers to block access to information at their absolute discretion without any safeguards, judicial or other independent supervision, due process provisions, limits to scope or duration and in a disproportionate manner, all of which are anathema to the principles enshrined in the Convention and international best practice.

In effect, these Models are establishing legislative provisions in countries which will eventually act as a bulwark or at least an obstruction to accession to the Convention and effective cross border cooperation. Once public authorities in countries become accustomed to the ease and effectiveness of such unbridled powers unhindered by safeguards (obstructive of accession though the powers may be) it will be a challenge, if not next to impossible, to persuade them to develop political will to undermine their own authorities and roll back such provisions. In this respect such Model Laws pose a significant risk to future progress in approving requests for accession from developing countries that may have implemented provisions based upon these Models.

The Models deliberately deviate from the Budapest Convention and the Commonwealth Model law by:

- Inserting controversial concepts and values such as those visible during the WCIT
- Attempting a forced demonstration of inadequacy of the Budapest Convention by (openly advocated in their workshops) inserting 'improvements' to undermine the credibility of the Convention, and advocating thereby for an 'improved' Cybercrime Treaty.

Whilst they go a long way to create new and unique offences related to cybercrime they do not include important provisions such as digital copyright as an offence (Article 10 of the Convention) and two of the models do not include Corporate Liability (Article 12 of the Convention), whilst the important definition of subscriber information is missing from all three.

From a cursory look at the Models they appear to follow the Commonwealth Model law (based on the Convention) and thus, appear to coincide in structure with many of the provisions of the Convention. However, on a closer examination it becomes clear that inexperienced tinkering with language has diluted the efficacy and limited the application of the offences and powers with edits that make the provisions technically and legally unsound.

They deviate from the Convention both in terms of the definitions, ingredients of offences established as best practice as well as redefining the scope of cybercrime to include criminalizing defamation of religion, blasphemy, insults, and any form of pornography, SPAM and a unique concept of "Illegal Remaining" without any carve outs, exceptions or safeguards. In this regard they are unsafe models of practice shrouded in the myth that they represent best practice of the EU and ITU member states.

So links provided by for instance, an online search or any videos deemed to be pornography or blasphemy or insulting or annoying, which under their provisions would constitute making available and procuring, while caching any images for a search result would additionally also constitute possession of such criminal material by a search engine. Even if such material (blasphemous, religious, insulting) was legal in most countries, if it is deemed to be illegal in the country in question, this Model would ensure criminalization across borders of online providers by such a territory, which would then seek cross border cooperation for enforcement of these provisions. Failure to cooperate by members of the Convention would be confusing for countries that adopt these models since these provisions would have been 'sold' to them as representing international best practice under the auspices of the EU. It also criminalizes SPAM even if there is only one recipient of a mail. They also criminalize cyberstalking, described as "annoying or insulting messages." Each of these categories are poorly defined and overly broad in application.

Notably, they criminalize any failure by a provider (regardless of jurisdiction) to take down any information regardless of its legality. Effectively, administrative authorities have absolute discretion to seek removal of any information or content whether legal or illegal or be subject to criminal liability. The providers subject to such criminal sanction are unique and include absurd definitions of hyperlink providers, search engine providers, hosting providers and access providers which are technically and legally incorrect, confusing, ambiguous, overlapping and so broad that they could include homes and individuals. Countries adopting these provisions, which have been told represent best practice, will expect that members of the Convention assist in compliance with such orders cross border and seek law enforcement cooperation against providers of State parties to the Convention.

They provide little or no indemnity, safe harbor or protections for intermediaries and service providers. Moreover, they attempt to criminalize activities and assign responsibilities to service providers in ways that would directly contradict protections outlined for companies under section 230 of the US Communications Decency Act and the EU E-Commerce directive. Basically an intermediary -- even ones located outside the jurisdiction of a state -- would be subject to these provisions, and could be held liable unless they strictly comply with the orders of any public authority.

These Model Laws looks to redefine many aspects of online crime, intermediary liability and Internet jurisdiction with overreaching provisions. Most importantly, their inexperienced attempts at editing the language of the Convention and the Commonwealth Model law have a significant diverging effect. They contain overly broad and ambiguous definitions of crimes which are open to unsafe and arbitrary interpretation and have a disproportionate focus on regulation and penalty without the necessary safeguards and protections for human rights required under international law and Article 15 of the Convention.

The following are summaries of each of the three ITU Model Laws:

3.2 HIPCAR

3.2.1 Summary

The HIPCAR Model Law is an edited version of the Commonwealth Model Law. However, substantial amendments to the Commonwealth language as well as insertion of unique and unsafe provisions have been made in the model which are both technically and legally incorrect language. For instance, for each offence it establishes a criteria of the conduct having been in "excess of a lawful excuse or justification". This language is obviously grammatically as well as legally and technically incorrect. One can exceed authority or powers, but an excuse or justification cannot be exceeded. This language appears to be a poor attempt at a forced edit in an attempt to replace the concept of "without right". This demonstrates the lack of skill over both the English language as well as drafting legislation. Moreover, the HIPCAR Model is heavily technology specific and establishes several purportedly new/innovative definitions and offences that are already covered under the conduct criminalized by the Convention. Apart from being generally fraught with failed attempts at innovation, poor language and drafting, technically and legally incorrect and overreaching provisions, it is unsafe. In many respects it over criminalizes and in others under criminalizes, contains overly broad and ambiguous offences which are open to unsafe and arbitrary interpretation. It attempts to invent offences and invent categories of service providers hitherto unknown in the legislative space[16], which are unique, overlapping, redundant and at times border on the absurd. It attempts to invent an offence of "Illegal Remaining" which relates to conduct after the initial illegal access of the computer system. The offence considers the conduct of remaining logged in by the offender without any further action or consequence to be an aggravated offence of illegal remaining. It also establishes the continuing use of the computer system (which is redundant being already covered under illegal data access) as an 'illegal remaining'. Similarly, it attempts to establish a new offence of data espionage, the language of which is technically and legally incorrect but also provides little utility being defined as language "computer data which are not meant for him". This forced innovation is redundant since the conduct is already covered under illegal access, illegal data interference, illegal interception, illegal system interference etc.

It also inappropriately and disproportionately criminalizes all forms of SPAM through a brief provision, whereas SPAM is a far more complex regulated commercial activity which merits a holistic, independent and self-contained legislation such as the US CAN-SPAM Act and the Singapore legislation[17]. The provision relates to the sending of electronic mail messages (which has the circular definition of communication using a unique electronic mail address, possibly excluding nontraditional messages, even if it is one message i.e. one message with only one recipient (it does not require multiple mails, which is only a requirement for its second optional limb). There is also no clarification as to what consent or solicitation of the message may constitute. There is no carve out for legitimate commercial purposes subject to opt-out by recipients – basically reversing the principles of the CAN-SPAM Act rules.

Whilst it creates new and unique offences it fails to include important provisions such as digital copyright as an offence (Article 10 of the Convention), Corporate Liability (Article 12 of the Convention) and the definition of subscriber information.

The model does little to add to the procedural provisions and instead its edits to the Commonwealth Model Law language detract from the skeletal language of the Commonwealth Model. It has a disproportionate focus on content regulation and unbridled powers without the necessary safeguards and civil liberty protections necessary with respect to criminal

[16] Access Provider "providing an electronic data transmission service by transmitting information provided by or to a user of the service in a communication network or providing access to a communication network"
Hyperlinks Provider "enables the access to information provided by third person by providing……characteristic or property of an element such as symbol, word, phrase, sentence, or image that contains information about another source and points to and causes to display another document when executed"
Caching Provider "providing an electronic data transmission service by automatic, intermediate and temporary storing information, performed for the sole purpose of making more efficient the information's onward transmission to other users of the service upon their Request"
Hosting Provider "providing an electronic data transmission service by storing of information provided by a user of the service."
Search Engine Provider "operates a search engine that either automatically or based on entries by others creates and index of Internet-related content or makes available electronic tools to search for information provided by third party"

[17] http://statutes.agc.gov.sg/aol/search/display/view.w3p;page=0;query=Id%3A%22b81d86b6-20e4-4467-93ed-9c3901c55e73%22%20Status%3Ainforce;rec=0

investigation and prosecution as envisaged by the Convention. It includes no provisions with respect to international cooperation. Its greatest challenge, however, stems from its deviation and attempts to improve upon the language of the Convention whilst inserting unique new offences within the scope of cybercrime, the language of which border on technical and legal absurdities. The unique, overlapping, redundant (at times bordering on the absurd) definitions that create new categories of service providers[18] though incorrect are more importantly they create risks for third parties (violating Article 15 (3) of the Convention).[19] This situation is further aggravated by the fact that these service providers have also been exposed in the Model to liability that is the inverse of principles established by OECD work with respect to intermediary liability protection. The Model does away with indemnities, safe harbor or protections for intermediaries and service providers and reverses general exclusion of liability for intermediaries, turning them into a conditional exclusion. Intermediaries have also been made liable for constructive knowledge/notice of information that may be deemed illegal by a public authority. It also mandates a public authority to order an intermediary (even if it is outside the territory of the state with a gTLD domain) to remove any information and "prevent" uploading of any identified content (**regardless of its legality**) or be subject to criminal liability[20]. This in effect imposes upon intermediaries the **duty to actively monitor** and report. These obligations are without any exceptions, exigent circumstances or due process.

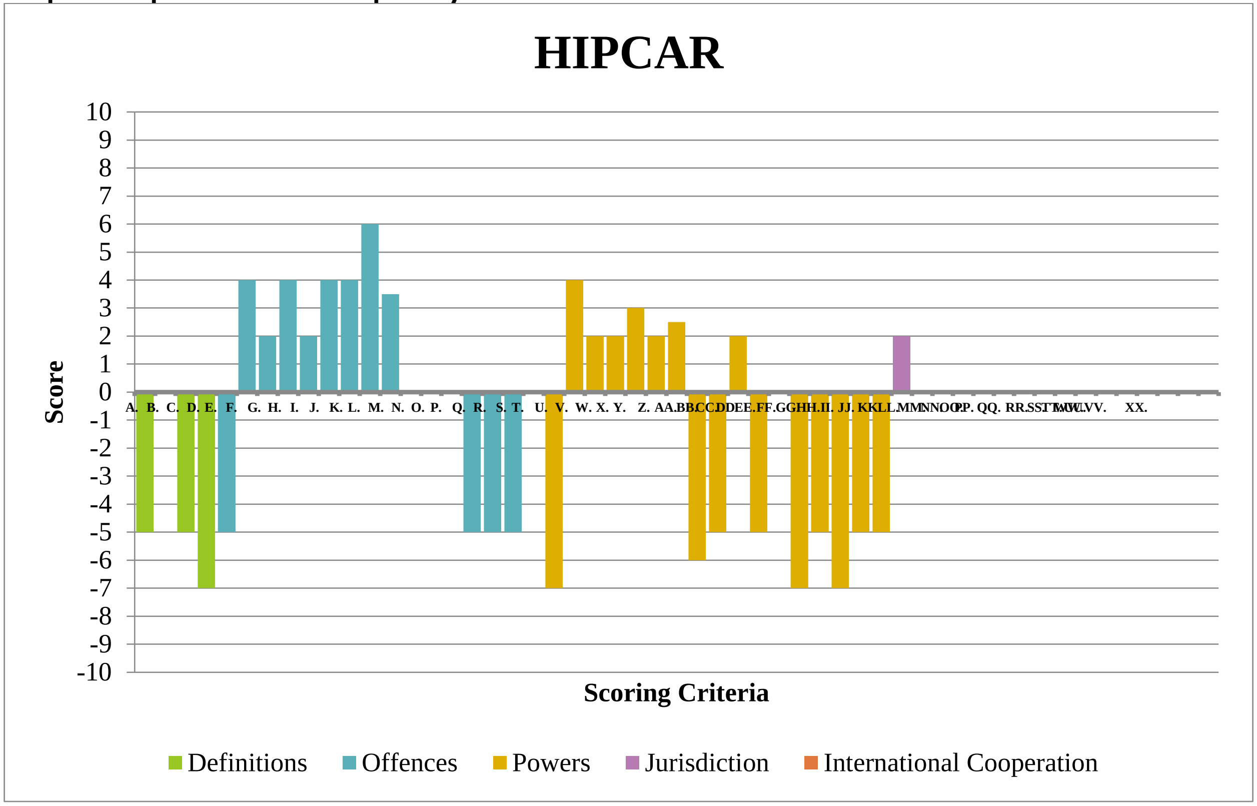
[18] See footnote 16

[19] "A.15 (3) To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties."

[20] is not liable for the information if

- the internet service provider expeditiously removes or disables access to the information after **receiving an order from any public authority or court to remove** the link; and
- the internet service provider, **upon obtaining knowledge or awareness** about **specific illegal information stored by other ways than an order from a public authority**, *expeditiously informs a public authority to enable them to evaluate the nature of the information and if necessary issue an order to remove the content.*

Graphical representation of Gap Analysis[21]



3.2.2 Examples of implementation

This is the most widely circulated and acknowledged draft of a cybercrime model law by the ITU. Its problematic provisions are present in existing legislation in St. Kitts and Nevis (St. Christopher and Nevis, Electronic Crimes Act, 2009 and its Electronic Transactions Act) and in the Jamaican Cybercrime Bill. St. Kitts' cybercrime law was the first to adopt HIPCAR (when still in draft) language[22] and its draftsman was appointed Consultant to the Jamaican Government[23] to review and harmonize Jamaican legislation with HIPCAR. It has also been used as the model in Bermuda for what is a pending Bill (was a Bill in mid 2012) and also extensively used in preparation of new legislation in Trinidad & Tobago whilst the Barbados legislation is more or less identical to HIPCAR. This "project has been conceived by ITU, the Caribbean Community (CARICOM) Secretariat and the CTU in response to requests from CARICOM States and other ICT stakeholders who saw the need for a more unified approach to the subject"[24]. It has been lobbied and advocated with much success by the Caribbean Telecommunications Union (CTU) and is accepted in CTU circles as the Model for the Caribbean and is part of the CTU's Strengthening the Policy and Institutional Framework[25].

[21] For Scoring Table and criteria see Annex A

[22] In particular section 3 (HIPCAR Jurisdiction), section 14 (HIPCAR Harassment and ICB4P cyber stalking), Electronic Transactions Act's sections 31-36 (Intermediary/ISP Liability – HIPCAR's access provider, caching provider, Hyperlink Provider (Information Location Tools), Monitoring and Compliance

[23] http://jamaica-gleaner.com/gleaner/20130125/lead/lead61.html

[24] http://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipcar/index.html

[25] "the recent ITU/HIPCAR Project in the region has gone some way in the developing of model policies and legislative text in area which are of significance to crime and security management, notably, Privacy and

3.3 HIPSSA

3.3.1 Summary

Under a second segment "the ITU and the European Commission (EC) [having] joined forces and signed an agreement (ITU-EC Project) aimed at providing "Support for the Establishment of Harmonized Policies for the ICT market in the ACP".[26] Interestingly the work on the Cybercrime Model Law is categorized under Cybersecurity.[27] It appears that the ITU though not having a clear mandate on cybercrime[28] worked on cybercrime legislation and model laws under its mandate for cybersecurity. HIPSSA is, with a few exceptions, identical to HIPCAR. The reach of this project throughout the African consentient is as impressive as its contents are disconcerting. Careful to avoid the politics of competing regional organizations[29] the ITU leveraged several regional bodies separately for dissemination and implementation of this Model Law. These include ECOWAS, ECCAS, CEMAC and SADC.

The Model suffers from the same infirmities as HIPCAR. Without repeating in detail the challenges posed by HIPCAR, it suffices to say that apart from being generally fraught with failed attempts at innovation, poor language and drafting, technically and legally incorrect and overreaching provisions, HIPSSA's provisions and drafting is unsafe. For details please see summary of HIPCAR. Differences between HIPCAR and HIPSSA extend to four aspects:

- A poor definition of 'access' has been included which states that access "means entering a computer system". Needless to mention this is both technically as well legally incorrect, quite apart from the fact that the dictionary meaning of term 'enter' is insufficient to define access. Regrettably, none of the model laws analyzed in this report include even a reasonably useful definition of the term 'access'. Most countries that have defined 'access' with some degree of efficacy have done so by emulating the UK's Computer Misuse Act which proves to be a far superior model in this respect.

- An offence related to Racist and Xenophobic material has been included which is helpful and based upon the Additional Protocol to the Convention. Unfortunately, the recurring poor attempts of the ITU-EC project to 'improve' upon the Convention once again lead to some complications. The definition of racism and xenophobia add the words "includes but is not limited to" making the definition redundant and nonspecific adding ambiguity and exposure to abuse of the provision. The inclusion of video and audio,

Data Protection, Interception of Communications, Cybercrime and Access to Information. These, once adopted
across the region should significantly improve the legislative framework for crime and security management." - http://www.ctu.int/attachments/084_CTU%20Project%20%20-%20Final%20Draft%20Policy%20Framework%20%20MThomas%20July%2028.pdf

[26] Harmonization of ICT Policies in Sub-Saharan Africa - Computer Crime and Cybercrime: Southern African Development Community (SADC) Model Law ["HIPSSA"] @ page I - http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/sadc_model_law_cybercrime.pdf

[27] http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Pages/default.aspx

[28] https://www.itu.int/osg/csd/cybersecurity/WSIS/RESOLUTION_130.pdf

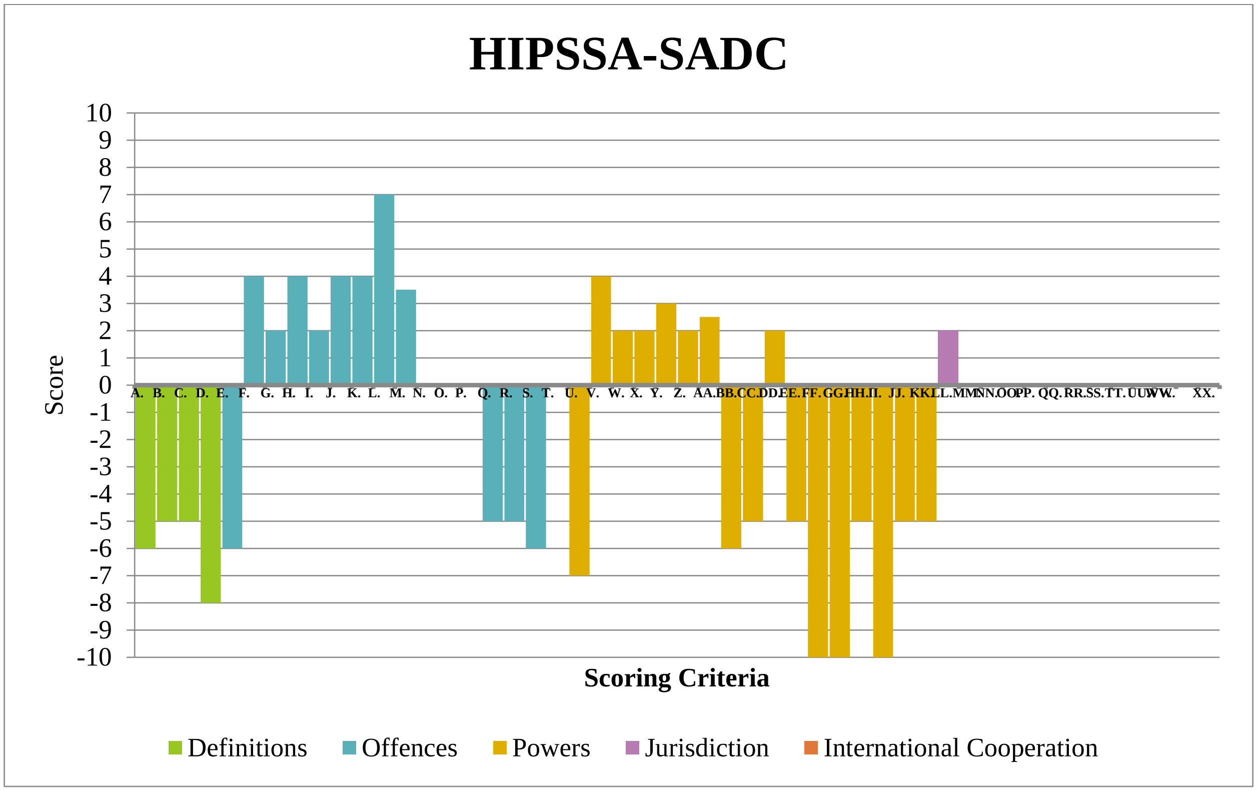
[29] "taken into account these very sensitive issues to avoid potential competition between the regional organizations" - http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Pages/default.aspx

which was unnecessary since it was already covered by the definition, is another change but due to a typo the comma between video and audio now reads "video audio recording" raising questions as to whether the recording must be both, or either video or audio. The offence itself attempts to implement the essence of Article 3 of the Protocol but overreaches and extends the offence to the transmission of such material without the caveat that it be transmitted for the purpose of distribution or making available. In doing so a private transmission not for the purpose of distribution or making available to another and a transmission by a service provider without knowledge of the content of the material have both been criminalized, possibly unintentionally, due to inexperienced drafting.

- Additionally, the Model also adds the offence of Racist and Xenophobic Insult (Article 5 of the Protocol) and Denial of Genocide and Crimes Against Humanity (Article 6 of the Protocol). These inclusions are simple reproductions of the provisions of the Protocol and are helpful inclusions though they suffer from ill-advised attempts to 'innovate' with the definition of racism and xenophobia.

- Helpfully, the Model also adds a provision enabling admissibility of electronic evidence for criminal matters.

Graphical representation of Gap Analysis[30]



Having said this, the Model still suffers from all the unfortunate infirmities of HIPCAR which it uses as its model.

[30] For Scoring Table and criteria see Annex B

What is also noteworthy is that though this purported Model Law is called the SADC Model Law on the ITU's website, no mention of the SADC Model Law was identifiable from a study of the SADC's official website. This again raises the concern and need for development and advocacy of Model Legislation through international bodies be subject to an official, formal and negotiated inter-governmental process, which HIPSSA appears to lack.

3.3.2 Examples of implementation

Though it has been challenging to access information for the purpose of comparing national legislation with HIPSSA, we have identified the Kenyan Cybercrime and Computer Related Crimes Bill of 2014 and the Tanzanian Computer Crime and Cybercrime Bill of 2013 included several provisions that are almost identical to HIPSSA. Uganda's Computer Misuse Act of 2011 and Mauritius' Computer Misuse and Cybercrime Act of 2002 though not identical in large part to HIPSSA have adapted and included certain provisions from HIPSSA.

3.4 ICB4PAC

3.4.1 Summary

This is the third segment of the ITU APC Project for largely Pacific Island states.[31] Most of the drafting and support is centered in Fiji from where a small group of draftsmen led by an ITU consultant (see HIPCAR) using the HIPCAR Model as the main format have modified and arrived at this draft which has important distinctions from the HIPCAR Model. Many of the deviations away from HIPCAR in this Model are the outcome of former draftsman from the Pakistani Ministry of IT & Telecom, responsible for the repealed Cybercrime legislation, as a result of stakeholder advocacy. Several provisions of Pakistan's repealed legislation are reproduced as a result. In most part it is these changes that distinguish ICB4PAC from HIPCAR. In many respects it overcriminalizes and in other respects undercriminalizes. It contains overly broad and ambiguous offences which are open to unsafe and arbitrary interpretation.

Apart from the challenges posed by HIPCAR's (see above) being a model for ICB4PAC, the latter proceeds to further 'innovate' and establish new and unique offences as cybercrimes. Unfortunately, it reads less like a model offence and more of a vague undefined political statement. For instance when criminalizing Illegal Gambling the only guidance it provides is that "A country may criminalize illegal online gambling". This is dangerous especially when vague terms such as religious offences are established by the Model. The offence simply states, "A country may criminalize ……. religious acts committed by using means of electronic systems." The ITU Consultant who drafted the Model when asked to advise the Government of Pakistan in the stakeholders consultation meeting clearly stated that this Model was most appropriate for developing countries since it specifically allowed (unlike the inadequate Convention) the criminalization of blasphemy on the internet.

These include the following:

- Cyberstalking – which criminalizes "annoying or insulting messages." The definition sets out some of the circumstances and stops short at annoyance (though by itself an overbroad term) which without identifying the conduct (language or suggestions), the

[31] http://www.itu.int/ITU-D/projects/ITU_EC_ACP/icb4pis/

purpose or the conduct that aggravates beyond what would be a civil matter[32], elevates it to the level of a crime.

The definition attempts to deal with a very serious and complex issue requiring careful definition and sufficient safeguards in order to avoid abuse, damaging legitimate commercial activity and curbing free speech in a manner that is non serious and attempts to cannibalize insufficiently, terms taken from legislations that deal with harassment online. Legislations that have dealt with this issue utilize the language used in this definition to only define the mens rea with respect to online harassment and do not by themselves define the entire conduct which has been criminalized for instance the closest use of the language comes from the Arizona criminal code which uses the language in the definition in conjunction with the conduct of using obscene lewd or profane language or suggest such an act or threaten physical harm to a person or their property. However, other States in the US provide a higher threshold for criminalizing such conduct as a safeguard against abuse. Moreover, the definition of obscene is far narrower when used in the United States or similar jurisdictions when interpreted by the courts or in light of the first amendment or other free speech protections. Parachuting this language into a model law whilst not only stripping away the elements of conduct provided for in other legislations but also failing to provide safeguard language with respect to civil liberties and human rights protections tends to create a content control and censorship legislation which in the form provided is open to abuse and has little to do with cybercrime and more to do with content control and free speech. Were such a definition and offence to be included in a model law (especially if funded by the EU) it would be necessary that a suitable definition and language that provides safeguards and protections for civil liberties ought to be included. The definition and offence as currently drafted also enables blocking of content and criminalizing online platforms and providers without appropriate carve-outs.

- Pornography – the Model promotes the criminalization of all forms of pornography. When linked with the overbroad, confusing and overlapping definitions of the various providers established by HIPCAR the addition of this offence takes on new meaning. Any links provided by online providers such as search engines or any videos deemed to be pornography would constitute making available and procuring, whilst caching any images would additionally also constitute possessing by search engine and other providers or platforms of this criminal material. Even if such material was legal in most countries, if it is deemed to be illegal in the country in question, this Model would ensure criminalization across borders of foreign online providers in such a territory.

- Lotteries - It criminalizes any type of a lottery which could include competitions and draws[33].

- Defamation & Religious Acts – it establishes the offences of defamation[34], insult of religion and blasphemy of any kind[35] as a cross border offence.

[32] "cyber stalking" means repeated coercion, intimidation, harassment, insult or annoyance through electronic system or electronic devices;

[33] "Illegal Gambling 18. A country may criminalize illegal online gambling."

[34] "Defamation 20. A country may criminalize defamation committed by means of electronic system"

[35] "Racial and religious offences. 21 A country may criminalize racial and religious acts committed by using means of electronic systems."

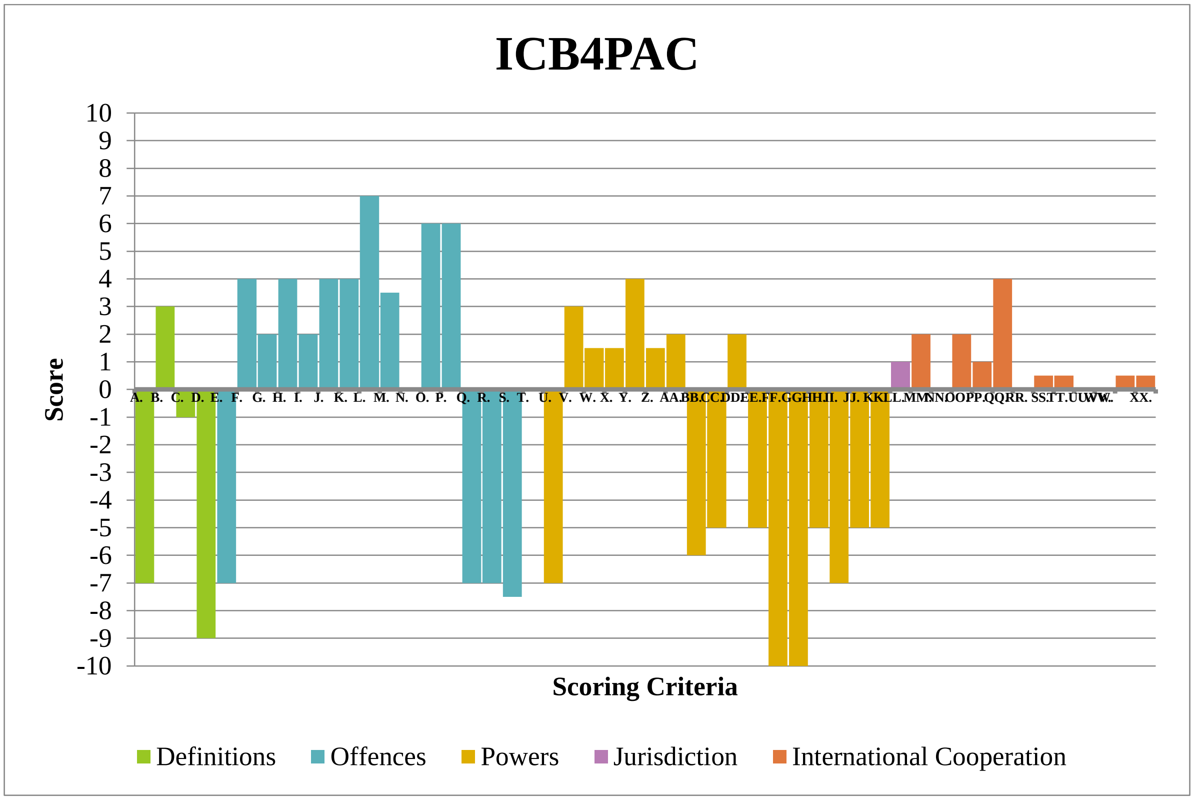
- Criminalization of single recipient emails as SPAM [36] & the criminalization of annoying/insulting messages as cyber stalking[37].

- Monitoring – as an encouraged option the Model establishes the possibility for positive and legally mandated across the board monitoring of all content.

It is critical to note that ICB4PAC is the only Model of the three that also includes one general provision that attempts to enable international cooperation in connection with these 'exotic' offences enabling the extraterritorial application of these offences for which the recipient countries will expect reciprocal enforcement having in their minds followed an EU sponsored model law. Finally, the Model establishes the possibility for positive and legally mandated across the board monitoring of all content.

By establishing absolute religious offences of defamation of religion, blasphemy, insults, simple pornography, without any carve outs, exceptions or safeguards the model overcriminalises and introduces offences with cross border application that would automatically criminalize much of the services offered by online platforms and providers.

Graphical representation of Gap Analysis[38]



[36] "(19) "*Spam"* means the unsolicited transmission of a harmful, fraudulent, misleading or illegal electronic mail message to any person or causing an electronic system to show such message for commercial purpose."

[37] "(3) "cyber stalking" means repeated coercion, intimidation, harassment, insult or annoyance through electronic system or electronic devices;"

[38] For Scoring Table and criteria see Annex C

3.5 Examples of implementation

There is little information available as to the actual implementation into Bills or existing legislation of the Model. From the data obtained as part of research for this paper from sources available online, it appears that the legislations of Tonga, Samoa, Fiji, Kiribati and Papua New Guinea have not as yet adopted this Model. Whether there are draft Bills underway to implement the model is unclear. According to the Knowledge based report, "The resulting draft assessment report was reviewed, discussed and adopted by broad consensus by participants at the first workshop to discuss and agree its findings (Vanuatu, March 2011)."

3.6 Collective Analysis of Strengths and Weaknesses of the ITU Model Laws & Their Impact

Strengths:

- The models, especially their framework are largely based upon the Commonwealth Model Law which was based upon the Convention and as such create a recognition for the enduring nature of the Convention as the source of best practice adopted even by the ITU.
- The models identify (though with some poorly edited changes to language) most if not all of the offences and powers and procedures enumerated in the Convention allowing at least the concept of these provisions and their importance to be impressed upon States and stakeholders.
- The models create awareness among political and other policy decision makers in States with respect to the need for a specialized cybercrime law.
- The models at least give a point of reference to begin engagement with States aware of the models when initiating capacity building or discussions with respect to accession.
- The models do adopt language with respect to misuse of devices (Article 6), e-forgery (Article 7), e-fraud (Article 8), which is consistent with the Convention. The Commonwealth Model Law for instance, though a better model does not include e-forgery and e-fraud.

Weaknesses:

- It would be redundant to list the various weaknesses and challenges posed by these models. However, their cumulative and strategic impact does create considerable challenges for a globally consistent, compatible and cooperative effort to combat cybercrime. Even amongst one another the three models, due to their substantial differences, do a disservice to the effort of harmonization and to promoting greater consistency, compatibility and convergence between national legislations on cybercrime. For instance, with the exception of the brief mention of international cooperation in ICB4PAC, both HIPCAR and HIPSSA make no mention of and thus, do little to promote introduction of international cooperation provisions into national law. ICB4PAC stands alone with the myriad of 'exotic' offences added to the already unique offences established by HIPCAR and HIPSSA. Ironically, though the ITU-EC Project is meant to establish "harmonization of….legislation" it does quite the opposite within the three regions it aims to influence and in relation to the global standards in relation to cybercrime. The inconsistencies between the three tend to promote divergence rather than harmonization, compatibility and convergence thereby impeding international cooperation. Most importantly they leave developing countries who have spent time and effort in this exercise short changed when it comes to the development and implementation of international best practice cybercrime legislation.

- The ITU, through this project, may to have extended its mandate and developed legal texts on cybercrime under the title of Cybersecurity.
- HIPCAR[39] is described under the title Cybercrime & **Cybersecurity** as "Model **Policy Guidelines** & Legislation **texts**"
- HIPSSA[40] is described under the title of **Cybersecurity** as the "**SADC** Model Law on Cybercrime", and
- ICB4PAC[41] is described under the title Cybercrime as a **"Knowledge-based report** (Skeleton)"

In the final analysis the importance of distinguishing between products that lack the quality and rigor of an official inter-governmental process and negotiation is key when assessing the credibility and efficacy of any document purporting to be a Model Law. The misperception of the credibility and sanction of the substance of the ITU Model Laws as bearing sanction and approval of the inter-governmental process indicated by the flags and emblems of the organizations placed on these documents is unsafe. It misidentifies the documents as representing international best practice.

3.7 EGRIP

3.7.1 Summary

Of all the Models analyzed in this paper, the World Bank-OECS-EGRIP Model Law on Cybercrime is by far the most unique and divergent. It is inconsistent with all known international models. Its language is divergent, technically and legally incorrect and appears to have been drafted without the benefit of specialized expertise in international best practice in the area of Cybercrime.

In essence, it includes only one recognizable cybercrime offence (illegal access), the language of which is inconsistent with any other model. Hence, all other cybercrime offences recognized in the Convention and other model laws are absent. Instead, the model over criminalizes and overreaches into conduct that is not cybercrime. In doing so it also uses language that apart from being technically and legally incorrect tends to epitomize poor legislative drafting. As an instance, the offence of violation of privacy[42] is described as "intentionally or knowingly captures, publishes or transmits the image of a private area of a person without his or her consent….."private area" means the **naked or undergarment clad genitals, pubic area, buttocks or female breast**". It also suffers from serious human rights and Article 15 deficiencies and violates free speech and other civil liberties without including safeguards.

Its status as an outlier is marked by the fact that even the ITU reportedly criticizes and disavows the model as representative of international best practice and advocates against its adoption. It provides no guidance on international cooperation whatsoever.

[39] Under the title Cybercrime & Cybersecurity as "Model Policy Guidelines & Legislation texts" http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPCAR/Pages/default.aspx

[40] Under the title of Cybersecurity as the "SADC Model Law on Cybercrime" http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Pages/default.aspx

[41] Under the title Cybercrime as a "Knowledge-based report (Skeleton)" http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/ICB4PAC/Pages/default.aspx

[42] A person who, intentionally or knowingly captures, publishes or transmits the image of a private area of a person without his or her consent, … "private area" means the naked or undergarment clad genitals, pubic area, buttocks or female breast"

3.7.2 Analysis of EGRIP

3.7.2.1 Definitions

Non- standard and technically incorrect

- Embellishment of definitions which are standard to international best practices creates restrictions which are inappropriate to legislation which aims to deal with electronic crimes. Inconsistent definitions create uncertainty as to their application under domestic law and in an international context where dual criminality may be required in order to extend and receive mutual assistance and international cooperation. The definitions of access, contaminant, data, electronic database, electronic device, electronic system, function, malicious code, plain version, service provider, source code and subscriber are non-standard.

Technology specific

- The use of technology specific language is restrictive and inappropriate to legislation that aims to deal with electronic crimes. Definitions which attempt to be technology specific are inaccurate and fail to be technically correct. Additionally such definitions risk becoming outdated and obsolete as new technology is developed. The definitions of function, malicious code and source code are technology specific definitions. As an example, the definition of source code includes listing of programs, electronic commands, design and layout and program analysis.

Technically incorrect

- Non-standard technically incorrect definitions fail to capture the meaning of terms in an electronic context, are vague and open to interpretation. The application of language which is not appropriate to electronic crimes is open to interpretation. As an example, the language 'halting' and 'choking' which have physical connotations in the definition of damage is problematic. The definitions of data, decryption, decryption information, encrypted data, encryption and plain version are technically incorrect and restrictive.

Ambiguous and uncertain

- The failure to define terms and use of vague language creates uncertainty. Ambiguous language and terms may result in uncertainty as to precisely what conduct is being criminalized. For instance, the definition of unauthorized access uses the term being defined within the definition itself. Further it is unclear what constitutes excess of authority.

Redundant and Inconsistent

- The use of duplicative definitions is unnecessary and creates uncertainty. The use of inconsistent terms creates problems in interpretation both in the domestic context as well as international cooperation. For instance the duplicative definitions of contaminant and malicious code and the use of the terms interchangeably creates confusion.

Use of specific case studies

- The use of case studies with reference to specific factual circumstances in definitions is also unhelpful, restrictive and has the result that conduct intended to be criminalized is not identified. This is evident from the definitions of access, contaminant, damage, data, electronic database, electronic device, electronic system, encryption, malicious code and source code. As an example the language 'virus, worm or Trojan horse' are specific examples used in the definition of malicious code.

Over criminalizing

- Over reaching definitions may have an over criminalizing effect and extend beyond the scope of electronic crimes legislation. As an example, the definition of subscriber is applicable to all users of services provided by a service provider, regardless of whether the user has subscribed to the services or not. As another example, the definition of service provider is so broad that even an employer may be deemed a service provider.

3.7.2.2 Offences

Missing corresponding provisions/ Inclusion of inappropriate provisions

- The EGRIP Electronic Crimes Bill does not have comparable provisions to international best practices and hence there would be not only gaps in the domestic law but international cooperation would be impacted. It only includes one section on some aspects of illegal access and interference [43] and there is no provision akin to interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system. This may pose problems both in terms of domestic hackers and additionally in terms of rendering assistance where dual criminality is required. As another example, offences related to infringements of copyright and related rights are not criminalized. This may have an adverse impact on domestic intellectual property rights and further, international trade.
- Conversely the offence of prank calls which has no nexus with electronic crimes is inappropriate to legislation which aims to deal with electronic crimes. Similarly, other conduct which does not constitute cybercrimes including offensive messages and communications[44], defamation[45], malicious code[46], violation of privacy[47], prank calls to LEAs[48], Electronic Stalking[49], Spoofing[50] and Unauthorized access to code[51] has been criminalized

[43] Section 4 of the Model

[44] A person shall not send by means of an electronic system or electronic device–…electronic mail or an electronic message for the purpose of causing **annoyance or inconvenience** ….. "electronic mail" or "electronic message" means a message or **information created or transmitted or received on an electronic system or electronic device including attachments** in text, images, audio, video and any other electronic record which may be transmitted with the message."

[45] "A person shall not **defame** another person using an electronic system under this this Act."

[46] "A person shall not write, offer, make available, distribute or transmit a **malicious code** through an electronic system."

[47] A person who, intentionally or knowingly captures, publishes or transmits the image of a **private area** of a person without his or her consent… "private area" means the **naked or undergarment clad genitals, pubic area, buttocks or female breast**;"

[48] "A person shall not make calls to any law enforcement authority or emergency services with the purpose of giving false and misleading information…**use a caller identification service to transmit misleading or inaccurate caller identification information service;"**

Missing elements

- Failure to include core elements of an offence may have the effect that the conduct which is intended to be criminalized is not an offence and there may be gaps within the domestic legal framework. This would also create an obstacle to international cooperation in instances where dual criminality is required. As an example, the offence of electronic fraud is missing the element of dishonesty. Notably, the EGRIP Electronic Crimes Bill also fails to include any carve out or safeguards for authorized testing and hence authorized conduct would be at par with illegal conduct.

Human rights protections

- Elements which would ensure that protection of human rights must be provided in order to safeguard human rights and civil liberties and would ensure consistency with international best practices. As an example, the requirement to comply with requests of law enforcement/police officers must ensure protection of the right against self-incrimination.

Ambiguous and uncertain

- The use of ambiguous language which fails to identify with certainty what conduct is criminalized is inappropriate to criminal legislation which establishes penalties including fines and imprisonment for such conduct. As a result such provisions may be open to interpretation and abuse. For instance the offence of sending offensive messages through communication service fails to provide any clarity with respect to what constitutes 'grossly offensive' or 'menacing' information. This creates uncertainty and may have an over criminalizing impact. Similarly the offence of identity theft is missing language on what constitutes a unique identification feature and is hence, unclear and vague. Although some guidance has been provided, albeit in the footnote to electronic defamation, the same is merely explanatory and does not serve as a substitute for a definition. As another example, the offence of violation of privacy is badly defined, may encompass offline acts and may raise questions with respect to the legality of CCTV. Further, the inclusion of an offence of electronic defamation which may be covered under the offence of defamation under existing domestic legislation may create inconsistencies, uncertainty and confusion.

Use of specific case studies

- Offences drafted to describe case studies with respect to specific facts fail to provide a legal definition of the conduct which is intended to be criminalized. As a consequence,

[49] "A person who, with intent to harass, intimidate, torment, **or embarrass** any other person, makes an electronic communication to such other person or a third party…Using any lewd, lascivious, indecent, or obscene words, images, or language, or suggesting the commission of any lewd or lascivious act anonymously or repeatedly whether or not conversation occurs"

[50] "A person shall not **establish a website or send an electronic message with a counterfeit source–**

(a) **with the intention that a visitor** to an electronic system or recipient of an electronic message will **believe it to be an authentic source**; or

(b) **to attract or solicit a person or electronic system**;

for the purpose of gaining unauthorized access to commit a further offence or obtain information which can be used for unlawful purposes.

[51] "A person shall not **disclose** or obtain a password, an access code or any other means of gaining access to an electronic system or data with intent to obtain wrongful gain or inflict wrongful loss to a person or for any unlawful purpose.

offences are restrictive and are only applicable to a particular set of facts. For example the offence of access and interference provides examples of conduct which may amount to interference rather providing a legal definition of the conduct which constitutes illegal access and interference.

Technology specific

- Technology specific offences risk becoming obsolete since offences which are not technology neutral are not sustainable. As an example, the offence of sending an offensive message over electronic mail rather than electronic communications may be restrictive and lead to inconsistency since sending an offensive email would be an offense but sending an offensive message via posting on a Facebook wall would not be covered.

Legally incorrect

- Legally incorrect language creates uncertainty and may be over criminalizing. For example, electronic stalking uses the terms torment and embarrass which are separate and distinct from harassment.

Technically incorrect

- Sending offensive messages through communication service, malicious code, electronic stalking, and spoofing are technically incorrect offences. As an example, the use of language such as a counterfeit source in the offence of spoofing is technically poor and somewhat inaccurate.

Over criminalizes

- Many offences under the EGRIP have a lower threshold of mens rea in comparison with international best practices and may be over criminalizing. As an illustration, the mens rea for the offence of access and interference is knowingly, whereas the mens rea for the offence of illegal access under international best practices is intention.
- The use of broad language is inappropriate to criminal legislation which needs to be very specific so that it is not vague or over criminalizes. The actus reus needs to be specific in order to avoid over criminalization. The language of 'enter into a relationship' in the offence of electronic fraud is unclear and over criminalizing. As another illustration, the insertion of the term text in the section on child pornography may also be problematic and encompass literary works. Although an attempt at a carve out has been made, the broad and vague language used would be open to interpretation which may in turn lead to inconsistencies in application. The provision also extends beyond pornography and encompasses solicitation and abuse.
- With respect to certain offences, brief language is provided. As an example, with respect to the definition and offence of defamation the sparse language used to define the offence of defamation may be open to over criminalization or at the very least ambiguity and uncertainty as to what constitutes defamation over the internet. The question of the scope of defamation may arise and whether the establishment of such an offence is an appropriate method of tackling the conduct intended to be criminalized.

Redundant

- The establishment of separate offences which criminalize the same conduct is redundant and may create uncertainty and problems with respect to interpretation. As an example the offences of electronic fraud, electronic forgery and spoofing significantly overlap with one another.

3.7.2.3 Powers & Procedures

Missing provisions

- Provisions on powers and procedures enabling preservation, disclosure and collection of evidence and facilitate international cooperation are absent and may result in inadequate powers and procedures. Further, international cooperation would be impacted. As an example, no provision akin to interception of content data is provided and obtaining evidence and prosecuting offences may be restricted on account of the absence of this power.

Missing essential elements

- The power of access search and seizure is missing the elements of copy, maintain integrity. It is unclear how a power to inspect and check the operation of an electronic system is either helpful or required. As another example, although service providers are not liable for disclosure of information to law enforcement, intermediary liability protection is missing.

Human rights and civil liberties

- The absence of limits on the scope and unclear limits on the duration of powers may create concerns with respect to civil liberties and human rights. Powers of arrest without a warrant does not include any grounds and raises similar concerns.

Uncertainty

- The use of vague language is also open to interpretation and abuse. For instance, the use of the term public interest in the provision on limited use of data and information is subjective and open to interpretation. Additionally there may be uncertainty as to their application and scope of certain powers. For instance the preservation order does not mention upon whom such an order would be served and applicable. Other safeguards, for instance the requirement for grounds for the application of powers and limits on the scope and duration of such powers are not provided with respect to the disclosure of preserved data order, production order, powers of access, search and seizure for the purpose of investigation, real time collection of traffic data, mobile phone tracking, deletion. Additionally the requirements for compliance with requests by law enforcement/police officers must ensure that the protection against self-incrimination is not violated.

Inappropriate

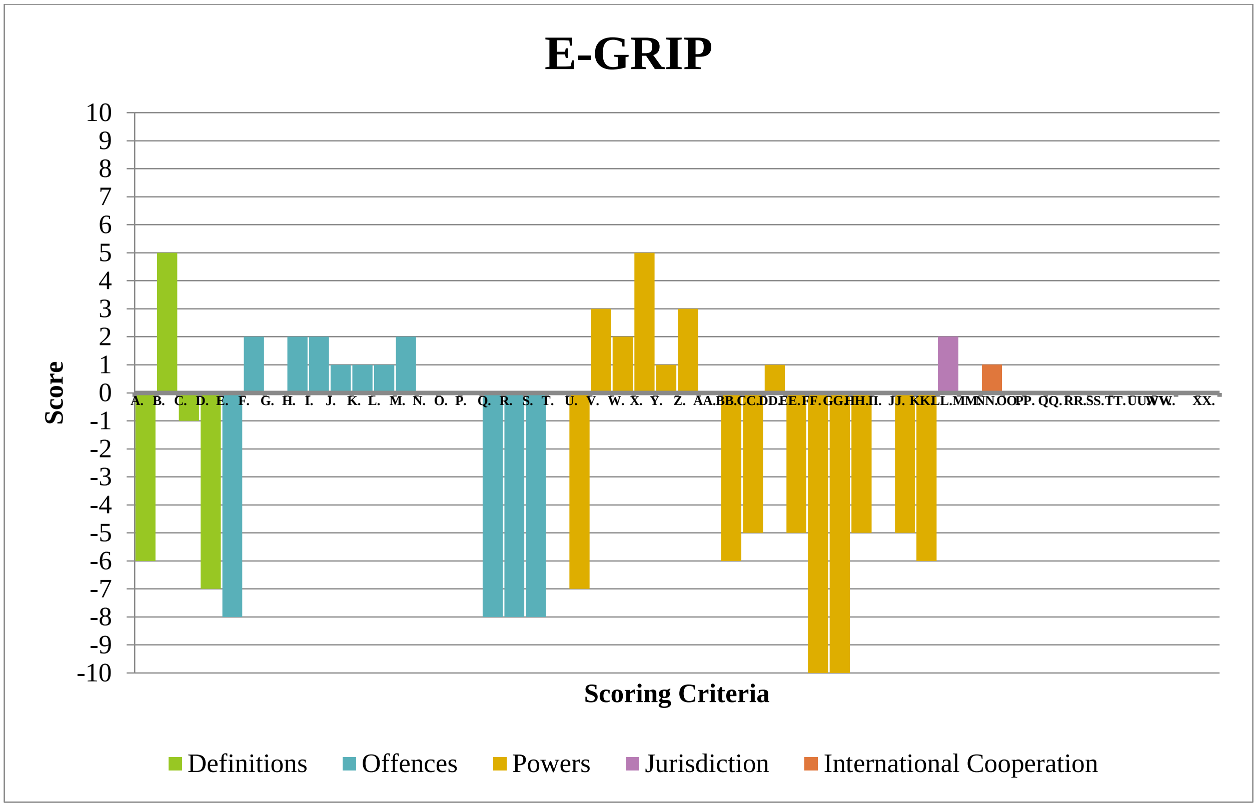
- The insertion of certain provisions are inappropriate to powers. As an instance, the provision which enables a police officer to delete or destroy material rather than access or seize or similarly secure the data and present the same to the judge for a determination as to whether the data is 'indecent'[52]. Similarly the provision on mobile phone tracking in the cases of events which have no link with electronic crimes is inappropriate. The ability of a judge to order deletion of allegedly indecent material in the absence of mention of grounds for such deletion is not consistent with requirements for investigation and prosecution.

3.7.2.4 International cooperation

Missing Provisions

- The EGRIP Electronic Crimes Bill does not include provisions for spontaneous information, expedited preservation of stored computer data, expedited disclosure of preserved traffic data, mutual assistance regarding accessing of stored computer data, trans border access to stored computer data, mutual assistance in the real time collection of traffic data, mutual assistance reading the interception of content data or 24/7 networks hence international cooperation in prosecution of electronic crimes is not enabled.

Graphical representation of Gap Analysis[53]



3.7.3 Examples of implementation

Our study reveals that Granada and Dominica have already adopted the EGRIP as a model for their Cybercrime Bills. Given its ownership by the World Bank and the OECS discussions with Eastern Caribbean nation officials suggests that there is a strong political will to uniformly adopt the model into national legislation throughout the Eastern Caribbean.

However, a recent Council of Europe mission to Dominica was able to identify EGRIP as the source of Dominica's poorly drafted Cybercrime Bill. Meetings with CARIBNOG and other stakeholders appeared to generate interest amongst stakeholders to review the acceptability of the EGRIP as an appropriate model for the Eastern Caribbean. Dominica based upon assistance

[53] For Scoring Table and criteria see Annex D

rendered by the Coe, OAS and Commonwealth Cybercrime Initiative is now reviewing the Bill. Grenada is also recently reported[54] to have committed to remove certain clauses and amend their Bill based entirely on EGRIP.

3.8 Commonwealth Model Law

3.8.1 Summary

The Commonwealth Model Law is by far the better of all Models analyzed for this paper. Though it does not cover all aspects desirable for a holistic model law the aspects it does cover in terms of both framework and language are consistent with international best practice and the Convention.

It covers most offences and powers but fails to cover international cooperation. This absence is explained in the commentary as a result of expected amendments to the Harare Scheme which are now in effect. Unfortunately, the separateness of the Model Law and the Harare Scheme and their lack of availability and accessibility as a package limit their delivery and effectiveness as a holistic tool.

Prior to the ITU Model Laws the Commonwealth Model Law did play a useful role in guiding States to draft cybercrime legislation. Even the ITU Model Laws are largely based upon the Commonwealth Model (though with substantial and problematic changes). Regrettably due to the lack of advocacy of the Commonwealth Model it appears to have faded into obscurity over the years and has been eclipsed by the promotion and advocacy of the EGRIP Model Law (in the Eastern Caribbean) and the ITU Model Laws. The Model Law was not available on the Commonwealth website or through a Google search.

3.8.2 Analysis of the Commonwealth Model Law

When drafting cybercrime legislation, one of the fundamental terms that needs to be defined is 'access' and another is 'unauthorized'. The Model does not provide language or guidance to assist in defining these terms. Instead draftsmen have to have to look to other best practice legislation to seek guidance. The UK and Singapore provide useful definitions in this respect which have in fact been followed by several countries.

Usefully the Model introduces both levels of *mens rea* for offences, that of intention and recklessness. This ensures that offences are not necessarily overcharged due to the absence of offences with lower thresholds which prevents the accused from being charged with crimes where preliminary procedures such as bail may set higher thresholds. At the same time it also provides the prosecution a lower threshold of proof to meet their case and obtain a conviction, albeit for a lower sentence.

With respect to offences the Model excludes:

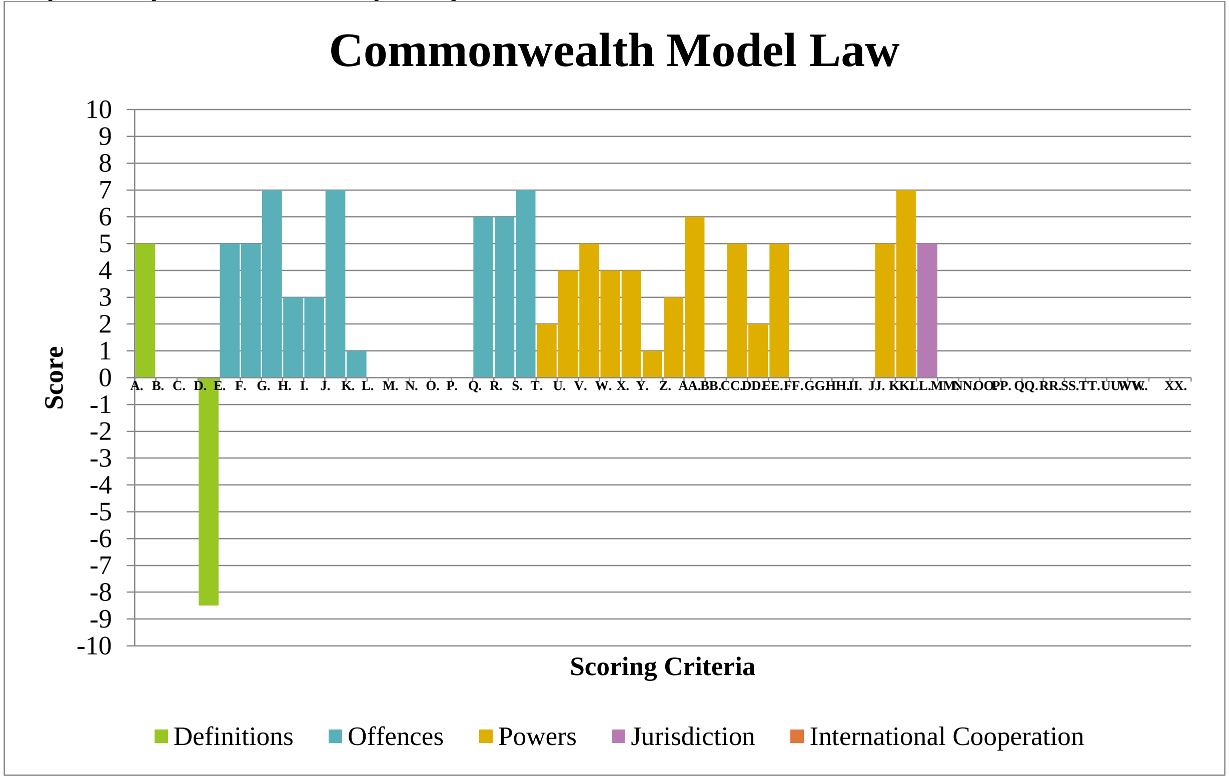
- E-forgery (Article 7 of the Convention)
- E-fraud (Article 8)
- Digital copyright/IPR protection (Article 10)

[54] http://grenadaadvocate.blogspot.com/2014/03/offensive-clause-to-be-removed-from.html
http://thenewtoday.gd/local-news/2014/02/16/nimrod-crime-bill-amended/

- Corporate liability (Article 12)

These both individually and cumulatively are substantial shortcomings of Commonwealth the Model Law. More so since the Model acknowledges being based upon the Convention but then gives no explanation for the reason for these exclusions depriving draftsmen of any guidance, possibly giving the impression that these provisions are not relevant and approving of such exclusion as a matter of international best practice.

Graphical representation of Gap Analysis[55]



In regards powers and procedures the Model is somewhat inadequate. They cannot be said to be sufficient in their language to adequately cover all necessary aspects related to the application for, supervision of and implementation of powers. The language is quite thin. For instance, instead of complying with Article 15 and specifying grounds for application for each power, the Model simply includes language such as "reasonable grounds" for each power depriving draftsmen from the guidance required to draft a holistic and Convention consistent (particularly with Article 15) provision for each power. The powers and procedures outlined in the Model do not include:

- Limitations on scope
- Limitations on duration
- Grounds justifying application for each power
- Intermediary liability protection provisions
- International cooperation provisions
- Adequate provision related to jurisdiction
- Adequate legislative language in general

[55] For Scoring Table and criteria see Annex E

- Adequate legislative language and procedural safeguards with respect to powers

The Model also does not include international cooperation provisions, though its commentary points to the Harare Scheme. This is unhelpful since there is no link to the document, particularly the latest version and tends to convey to a less informed audience the perception of international cooperation provisions being inessential.

Thus, the Model though better than the rest falls short of what is needed for a holistic, compatible and convergent cybercrime model law consistent with international best practice, particularly the Convention.

3.8.3 Examples of implementation

Instances where the Commonwealth Model Law has been used when drafting Cybercrime legislation include Tonga's Computer Crimes Act of 2003, Ghana's Electronic Transactions Act of 2008, Antigua's Computer Misuse Act of 2006 and others. However, due to the lack of advocacy and availability of the Model Law (removed from the Commonwealth website) as well as the increased advocacy of the alternative ITU Model Laws, the Model has been replaced in popularity by the ITU Model Laws in Commonwealth countries. Post 2007 we are unable to identify countries that have modeled their legislation on the Commonwealth Model Law as opposed to the ITU Model Laws. Another reason for the stagnation of the Commonwealth Model Law's uptake has been the limited focus and clarity of the Commonwealth Cybercrime Initiative in understanding the challenges posed by the ITU Model Laws to their own Model Law and therefore, placing their Model Law front and center as the primary action item in any project. Instead focus on National cybercrime and cybersecurity strategies and non-legislative and informal law enforcement cooperation appear to have overshadowed the primacy of the Model Law.

4 Conclusion

4.1 Collective impact of existing models

The use of such model laws poses risks and serious concerns. Absence of essential provisions, defective language, disjointed nature, infusion of unique, poor quality, peculiar and unsafe offences and their divergence away from and inconsistency with international best practice do a disservice to the goal of achieving greater international cooperation against cybercrime.

Countries and stakeholders confronted with texts that purport to be "Model Laws" and bear the emblem and flag of inter-governmental organizations tend to convey the perception that they have gone through the rigor and reflect the quality that is expected of a formal, negotiated inter-governmental process and hence, represent international best practice when in fact their credibility is at best unclear. This appears to be highly problematic especially in the instance where developing countries expend significant resources in terms of loans, grants and political capital on drafting legislation they expect would be consistent with international best practice only to discover that they are left with poor quality laws with little or no utility in terms of combatting cybercrime and international cooperation.

The Model Laws analyzed above adversely affect the harmonization of domestic law with international standards and best practice. They thus create barriers and reduce the readiness of many States to cooperate internationally against cybercrime.

Experience with the Model Laws discussed in this paper raises further questions as to the utility of Model Laws on cybercrime in general at present.[56] Use of the text of the Budapest Convention combined with actual examples of implementation by Parties to this treaty that are relevant to the legal system of a country seeking to reform its legislation coupled with its delivery in a form that is relatively accessible and comprehendible by recipient countries that may require capacity in this area, may be the more pragmatic way ahead.

4.2 Recommendations

In order to break through the noise resonating in many countries, particularly developing states, with respect to these Model Laws, what is likely necessary is a concerted and well-resourced outreach effort to advocate for the Convention and best practice with those countries beyond those that have requested or are in the process of requesting accession and to engage on legislation through specific capacity building efforts. This should assist recipient countries understand better the challenges posed by these Model Laws, which commonly form part of discussions with local stakeholders who may have Googled for tools in order to assist with drafting. It is also not uncommon (instead this is a consistent theme) when engaging with developing counties on legislation that their officials, particularly draftsmen requests specific assistance in drafting legislation and regulations on cybercrime and electronic evidence. This proves to be an opportunity which should be capitalized upon as part of a positive campaign in favor of the Convention.

Given the shortcomings of some of the model laws discussed in this paper, the adverse impact in particular on developing countries, and the confusion as regards their status, the Council of Europe may engage with the organizations to stir their work away from these model laws towards the Convention or at least towards a more neutral position that is more compatible with international best practice.

It may also be advisable that States seek clarification as to the status of model laws of the respective organizations of which they are members, in particular where there is an appearance that model laws have been formally endorsed by such organizations. In parallel, it may be useful to enter into dialogue with the organizations which appear to endorse such models. In the past, some organizations have removed similar documents[57]. Hence, it may be useful to either have such poor quality, unsafe and problematic documents removed from circulation or in the alternative, at least attempt to redact the emblems and purported statements of support of the various international organizations attached to the most problematic documents.

[56] Discussions at the UN Intergovernmental Expert Group on Cybercrime so far failed to reach consensus on the options related to preparing model cybercrime provisions as proposed in the draft study presented by the UN Office on Drugs and Crime in February 2013. http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

[57] ITU Toolkit for Cybercrime Legislation 2010

5 Appendix: Scoring tables for the Model Laws

5.1 Annex A: HIPCAR

Criteria Code	Scoring Criteria	Scores
A.	Article 1 Definitions	-5
B.	Definitions of access and authorization	0
C.	Impact on business/ rights holders	-5
D.	Compatibility of definitions for International Cooperation	-7
	Section 1- Substantive law	
E.	Overall legal and technical adequacy	-5
F.	Article 2 –Illegal access	4
G.	Article 3 –Illegal interception	2
H.	Article 4 –Data interference	4
I.	Article 5 –System interference	2
J.	Article 6 –Misuse of devices	4
K.	Article 7 –Computer-related forgery	4
L.	Article 8 –Computer-related fraud	6
M.	Article 9 –Offences related to child pornography	3.5
N.	Article 10 –Offences related to infringements of copyright and related rights	0
O.	Article 11 –Attempt and aiding or abetting	0
P.	Article 12 –Corporate liability	0
Q.	Absence of offences, inappropriate, technically incorrect or unsafe offences	-5
R.	Consistency with Human Rights (negative scores for regressive offences)	-5
S.	Compatibility of offences for International Cooperation	-5
	Section 2 – Procedural law	
T.	Applicability of procedural provisions to non-cyber offences	0
U.	Article 15 –Conditions and safeguards	-7
V.	Article 16 –Expedited preservation of stored computer data	4
W.	Article 17 –Expedited preservation and partial disclosure of traffic data	2
X.	Article 18 –Production order	2
Y.	Article 19 –Search and seizure of stored computer data	3
Z.	Article 20 –Real-time collection of traffic data	2
AA.	Article 21 –Interception of content data	2.5
BB.	Impact on Private Sector	-6
CC.	UNDHR/ ICCPR compliance	-5
DD.	Effective judicial supervision	2
EE.	Proportionality	-5
FF.	Grounds justifying application of powers	0
GG.	Limitation of scope and duration	-7
HH.	Privacy protection	-5
II.	Consistency with international best practice on intermediary liability protection (OECD)	-7
JJ.	Safeguards to protect third parties	-5
KK.	Compatibility of Powers for International Cooperation	-5

	Section 3 – Jurisdiction	
LL.	Article 22 –Jurisdiction	2
	Chapter III – International co-operation	
MM.	Article 23 –General principles relating to international co-operation	0
NN.	Article 24 –Extradition	0
OO.	Article 25 –General principles relating to mutual assistance	0
PP.	Article 26 –Spontaneous information	0
QQ.	Article 27 –Procedures pertaining to mutual assistance requests in the absence of applicable international agreements	0
RR.	Article 28 –Confidentiality and limitation on use	0
SS.	Article 29 –Expedited preservation of stored computer data	0
TT.	Article 30 –Expedited disclosure of preserved traffic data	0
UU.	Article 31 –Mutual assistance regarding accessing of stored computer data	0
VV.	Article 32 –Trans-border access to stored computer data with consent or where publicly available	0
WW.	Article 33 –Mutual assistance in the real-time collection of traffic data	0
XX.	Article 34 –Mutual assistance regarding the interception of content data	0
YY.	Article 35 –24/7 Network	0

5.2 Annex B: SADC

Criteria Code	Scoring Criteria	Scores
A.	Article 1 Definitions	-6
B.	Definitions of access and authorization	-5
C.	Impact on business/ rights holders	-5
D.	Compatibility of definitions for International Cooperation	-8
	Section 1- Substantive law	
E.	Overall legal and technical adequacy	-6
F.	Article 2 –Illegal access	4
G.	Article 3 –Illegal interception	2
H.	Article 4 –Data interference	4
I.	Article 5 –System interference	2
J.	Article 6 –Misuse of devices	4
K.	Article 7 –Computer-related forgery	4
L.	Article 8 –Computer-related fraud	7
M.	Article 9 –Offences related to child pornography	3.5
N.	Article 10 –Offences related to infringements of copyright and related rights	0
O.	Article 11 –Attempt and aiding or abetting	0
P.	Article 12 –Corporate liability	0
Q.	Absence of offences, inappropriate, technically incorrect or unsafe offences	-5
R.	Consistency with Human Rights (negative scores for regressive offences)	-5
S.	Compatibility of offences for International Cooperation	-6

	Section 2 – Procedural law	
T.	Applicability of procedural provisions to non-cyber offences	0
U.	Article 15 –Conditions and safeguards	-7
V.	Article 16 –Expedited preservation of stored computer data	4
W.	Article 17 –Expedited preservation and partial disclosure of traffic data	2
X.	Article 18 –Production order	2
Y.	Article 19 –Search and seizure of stored computer data	3
Z.	Article 20 –Real-time collection of traffic data	2
AA.	Article 21 –Interception of content data	2.5
BB.	Impact on Private Sector	-6
CC.	UNDHR/ ICCPR compliance	-5
DD.	Effective judicial supervision	2
EE.	Proportionality	-5
FF.	Adequacy of grounds justifying application of powers	-10
GG.	Limitation of the scope and duration	-10
HH.	Privacy protection	-5
II.	Consistency with international best practice on intermediary liability protection (OECD)	-10
JJ.	Safeguards to protect third parties	-5
KK.	Compatibility of Powers for International Cooperation	-5
	Section 3 – Jurisdiction	
LL.	Article 22 –Jurisdiction	2
	Chapter III – International co-operation	
MM.	Article 23 –General principles relating to international co-operation	0
NN.	Article 24 –Extradition	0
OO.	Article 25 –General principles relating to mutual assistance	0
PP.	Article 26 –Spontaneous information	0
QQ.	Article 27 –Procedures pertaining to mutual assistance requests in the absence of applicable international agreements	0
RR.	Article 28 –Confidentiality and limitation on use	0
SS.	Article 29 –Expedited preservation of stored computer data	0
TT.	Article 30 –Expedited disclosure of preserved traffic data	0
UU.	Article 31 –Mutual assistance regarding accessing of stored computer data	0
VV.	Article 32 –Trans-border access to stored computer data with consent or where publicly available	0
WW.	Article 33 –Mutual assistance in the real-time collection of traffic data	0
XX.	Article 34 –Mutual assistance regarding the interception of content data	0
YY.	Article 35 –24/7 Network	0

5.3 Annex C: ICB4PAC

Criteria Code	Scoring Criteria	Scores
A.	Article 1 Definitions	-7
B.	Definitions of access and authorization	3

C.	Impact on business/ rights holders	-1
D.	Compatibility of definitions for International Cooperation	-9
	Section 1- Substantive law	
E.	Overall legal and technical adequacy	-7
F.	Article 2 –Illegal access	4
G.	Article 3 –Illegal interception	2
H.	Article 4 –Data interference	4
I.	Article 5 –System interference	2
J.	Article 6 –Misuse of devices	4
K.	Article 7 –Computer-related forgery	4
L.	Article 8 –Computer-related fraud	7
M.	Article 9 –Offences related to child pornography	3.5
N.	Article 10 –Offences related to infringements of copyright and related rights	0
O.	Article 11 –Attempt and aiding or abetting	6
P.	Article 12 –Corporate liability	6
Q.	Absence of offences, inappropriate, technically incorrect or unsafe offences	-7
R.	Consistency with Human Rights (negative scores for regressive offences)	-7
S.	Compatibility of offences for International Cooperation	-7.5
	Section 2 – Procedural law	
T.	Applicability of procedural provisions to non-cyber offences	0
U.	Article 15 –Conditions and safeguards	-7
V.	Article 16 –Expedited preservation of stored computer data	3
W.	Article 17 –Expedited preservation and partial disclosure of traffic data	1.5
X.	Article 18 –Production order	1.5
Y.	Article 19 –Search and seizure of stored computer data	4
Z.	Article 20 –Real-time collection of traffic data	1.5
AA.	Article 21 –Interception of content data	2
BB.	Impact on Private Sector	-6
CC.	UNDHR/ ICCPR compliance	-5
DD.	Effective judicial supervision	2
EE.	Proportionality	-5
FF.	Adequacy of grounds justifying application of powers	-10
GG.	Limitation of the scope and duration	-10
HH.	Privacy protection	-5
II.	Consistency with international best practice on intermediary liability protection (OECD)	-7
JJ.	Safeguards to protect third parties	-5
KK.	Compatibility of Powers for International Cooperation	-5
	Section 3 – Jurisdiction	
LL.	Article 22 –Jurisdiction	1
	Chapter III – International co-operation	
MM.	Article 23 –General principles relating to international co-operation	2
NN.	Article 24 –Extradition	0

OO.	Article 25 –General principles relating to mutual assistance	2
PP.	Article 26 –Spontaneous information	1
QQ.	Article 27 –Procedures pertaining to mutual assistance requests in the absence of applicable international agreements	4
RR.	Article 28 –Confidentiality and limitation on use	0
SS.	Article 29 –Expedited preservation of stored computer data	0.5
TT.	Article 30 –Expedited disclosure of preserved traffic data	0.5
UU.	Article 31 –Mutual assistance regarding accessing of stored computer data	0
VV.	Article 32 –Trans-border access to stored computer data with consent or where publicly available	0
WW.	Article 33 –Mutual assistance in the real-time collection of traffic data	0.5
XX.	Article 34 –Mutual assistance regarding the interception of content data	0.5
YY.	Article 35 –24/7 Network	0

5.4 Annex D: EGRIP

Criteria Code	Scoring Criteria	Scores
A.	Article 1 Definitions	-6
B.	Definitions of access and authorization	5
C.	Impact on business/ rights holders	-1
D.	Compatibility of definitions for International Cooperation	-7
	Section 1- Substantive law	
E.	Overall legal and technical adequacy	-8
F.	Article 2 –Illegal access	2
G.	Article 3 –Illegal interception	0
H.	Article 4 –Data interference	2
I.	Article 5 –System interference	2
J.	Article 6 –Misuse of devices	1
K.	Article 7 –Computer-related forgery	1
L.	Article 8 –Computer-related fraud	1
M.	Article 9 –Offences related to child pornography	2
N.	Article 10 –Offences related to infringements of copyright and related rights	0
O.	Article 11 –Attempt and aiding or abetting	0
P.	Article 12 –Corporate liability	0
Q.	Absence of offences, inappropriate, technically incorrect or unsafe offences	-8
R.	Consistency with Human Rights (negative scores for regressive offences)	-8
S.	Compatibility of offences for International Cooperation	-8
	Section 2 – Procedural law	
T.	Applicability of procedural provisions to non-cyber offences	0
U.	Article 15 –Conditions and safeguards	-7
V.	Article 16 –Expedited preservation of stored computer data	3
W.	Article 17 –Expedited preservation and partial disclosure of traffic data	2
X.	Article 18 –Production order	5
Y.	Article 19 –Search and seizure of stored computer data	1
Z.	Article 20 –Real-time collection of traffic data	3

AA.	Article 21 –Interception of content data	0
BB.	Impact on Private Sector	-6
CC.	UNDHR/ ICCPR compliance	-5
DD.	Effective judicial supervision	1
EE.	Proportionality	-5
FF.	Adequacy of grounds justifying application of powers	-10
GG.	Limitation of the scope and duration	-10
HH.	Privacy protection	-5
II.	Consistency with international best practice on intermediary liability protection (OECD)	0
JJ.	Safeguards to protect third parties	-5
KK.	Compatibility of Powers for International Cooperation	-6
	Section 3 – Jurisdiction	
LL.	Article 22 –Jurisdiction	2
	Chapter III – International co-operation	
MM.	Article 23 –General principles relating to international co-operation	0
NN.	Article 24 –Extradition	1
OO.	Article 25 –General principles relating to mutual assistance	0
PP.	Article 26 –Spontaneous information	0
QQ.	Article 27 –Procedures pertaining to mutual assistance requests in the absence of applicable international agreements	0
RR.	Article 28 –Confidentiality and limitation on use	0
SS.	Article 29 –Expedited preservation of stored computer data	0
TT.	Article 30 –Expedited disclosure of preserved traffic data	0
UU.	Article 31 –Mutual assistance regarding accessing of stored computer data	0
VV.	Article 32 –Trans-border access to stored computer data with consent or where publicly available	0
WW.	Article 33 –Mutual assistance in the real-time collection of traffic data	0
XX.	Article 34 –Mutual assistance regarding the interception of content data	0
YY.	Article 35 –24/7 Network	0

5.5 Annex E: Commonwealth Model Law

Criteria Code	Scoring Criteria	Scores
A.	Article 1 Definitions	5
B.	Definitions of access and authorization	0
C.	Impact on business/ rights holders	0
D.	Compatibility of definitions for International Cooperation	-8.5
	Section 1- Substantive law	
E.	Overall legal and technical adequacy	5
F.	Article 2 –Illegal access	5
G.	Article 3 –Illegal interception	7
H.	Article 4 –Data interference	3
I.	Article 5 –System interference	3

J.	Article 6 –Misuse of devices	7
K.	Article 7 –Computer-related forgery	1
L.	Article 8 –Computer-related fraud	0
M.	Article 9 –Offences related to child pornography	0
N.	Article 10 –Offences related to infringements of copyright and related rights	0
O.	Article 11 –Attempt and aiding or abetting	0
P.	Article 12 –Corporate liability	0
Q.	Absence of offences, inappropriate, technically incorrect or unsafe offences	6
R.	Consistency with Human Rights (negative scores for regressive offences)	6
S.	Compatibility of offences for International Cooperation	7
	Section 2 – Procedural law	
T.	Applicability of procedural provisions to non-cyber offences	2
U.	Article 15 –Conditions and safeguards	4
V.	Article 16 –Expedited preservation of stored computer data	5
W.	Article 17 –Expedited preservation and partial disclosure of traffic data	4
X.	Article 18 –Production order	4
Y.	Article 19 –Search and seizure of stored computer data	1
Z.	Article 20 –Real-time collection of traffic data	3
AA.	Article 21 –Interception of content data	6
BB.	Impact on Private Sector	0
CC.	UNDHR/ ICCPR compliance	5
DD.	Effective judicial supervision	2
EE.	Proportionality	5
FF.	Adequacy of grounds justifying application of powers	0
GG.	Limitation of the scope and duration	0
HH.	Privacy protection	0
II.	Consistency with international best practice on intermediary liability protection (OECD)	0
JJ.	Safeguards to protect third parties	5
KK.	Compatibility of Powers for International Cooperation	7
	Section 3 – Jurisdiction	
LL.	Article 22 –Jurisdiction	5
	Chapter III – International co-operation	
MM.	Article 23 –General principles relating to international co-operation	0
NN.	Article 24 –Extradition	0
OO.	Article 25 –General principles relating to mutual assistance	0
PP.	Article 26 –Spontaneous information	0
QQ.	Article 27 –Procedures pertaining to mutual assistance requests in the absence of applicable international agreements	0
RR.	Article 28 –Confidentiality and limitation on use	0
SS.	Article 29 –Expedited preservation of stored computer data	0
TT.	Article 30 –Expedited disclosure of preserved traffic data	0
UU.	Article 31 –Mutual assistance regarding accessing of stored computer data	0
VV.	Article 32 –Trans-border access to stored computer data with consent or where publicly available	0

WW.	Article 33 –Mutual assistance in the real-time collection of traffic data	0
XX.	Article 34 –Mutual assistance regarding the interception of content data	0
YY.	Article 35 –24/7 Network	0