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

Cybercrime Model Laws

Zahid Jamil Esq.
Consultant
Jamil & Jamil
Barrister-at-law
Pakistan

www.coe.int/cybercrime

Funded
by the European Union
and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Implemented
by the Council of Europe

Model Laws – Discussion Paper

- Scope
- Findings
- Methodology
- Conclusions

Model Laws – Scope

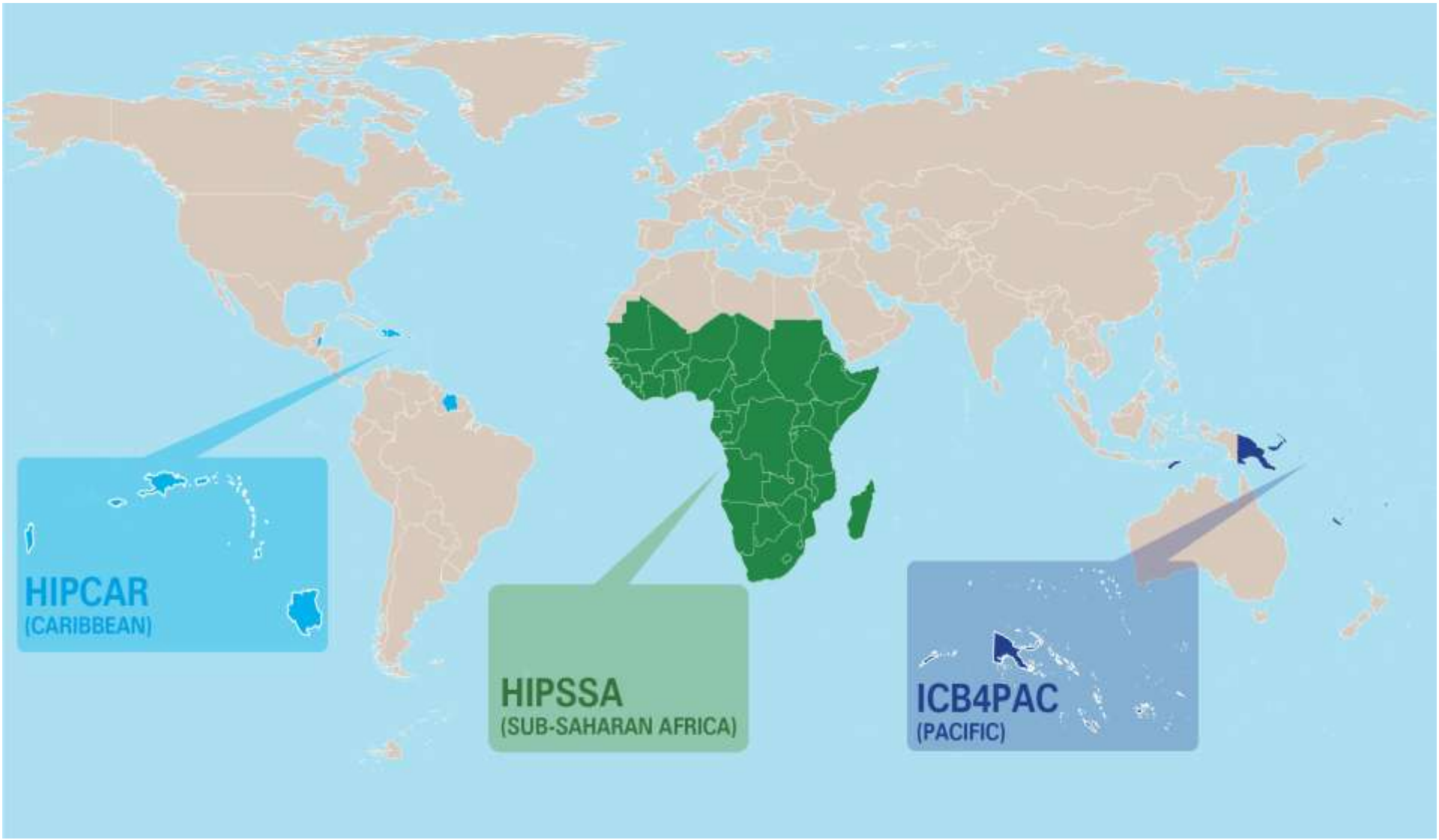
- Scope:
  - ❑ Existing Model Laws
  - ❑ ITU (HIPCAR, HPSSA, ICB4PAC)
  - ❑ World Bank OECS – EGRIP
  - ❑ Commonwealth

Model Laws – Methodology

- Comparison with Budapest Convention
- Comments
- ICB4PAC, EGRIP, Commonwealth

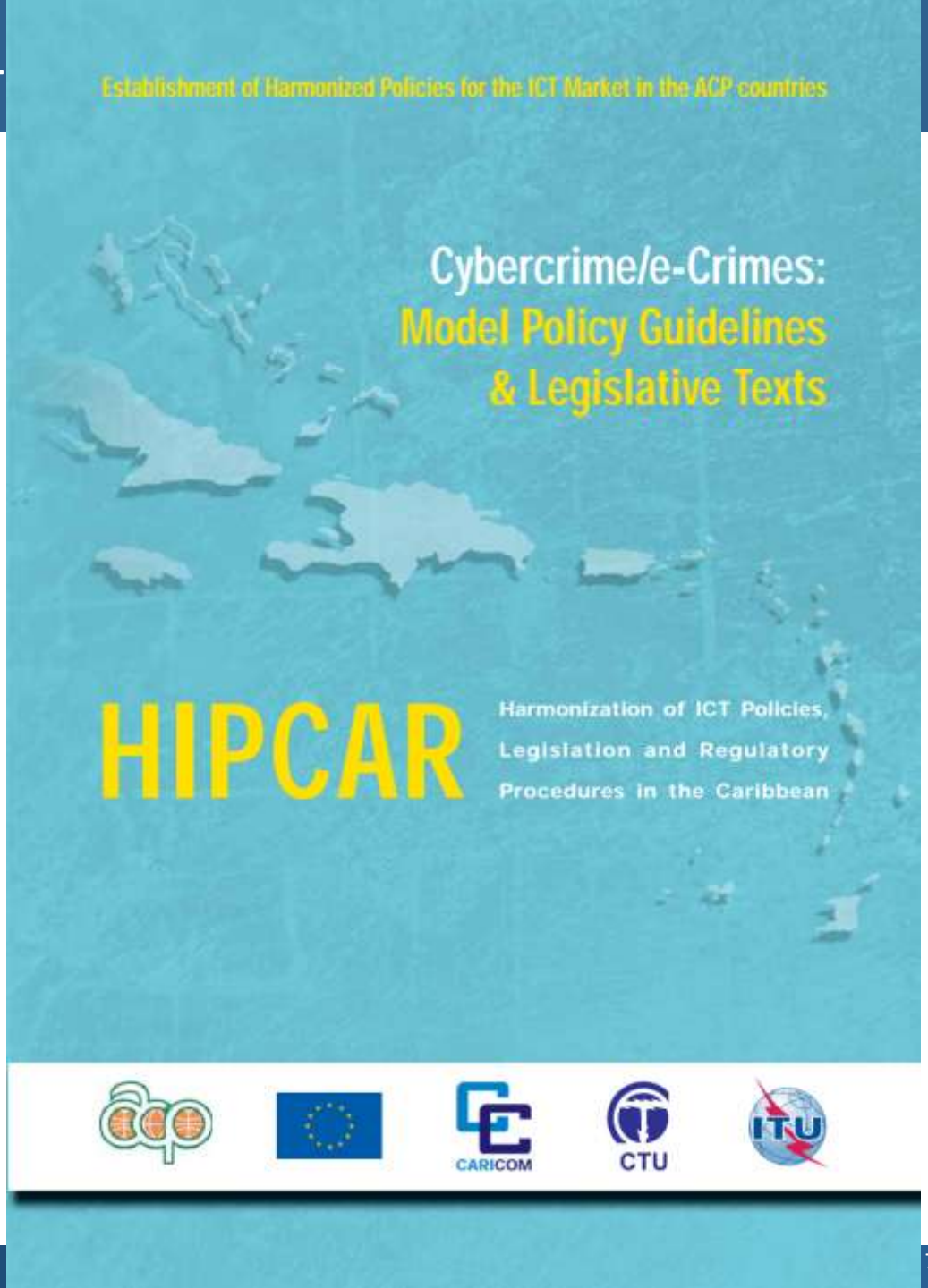
Model Laws –Findings- ITU Models

Model Laws –Findings– ITU Models



Model Laws –Findings– IT

- ITU: HIPCAR



Model Laws –Findings– ITU Models - HIPCAR

(BDT)
Place des Nations
CH-1211 Geneva 20
Switzerland

I. ICT legislative framework covering information society issues:

1. eCommerce - transaction
   - Assessment report
   - Model Policy Guidelines & Legislation texts [EN] [FR] [NL]
2. eCommerce - evidence
   - Assessment report
   - Model Policy Guidelines & Legislation texts [EN] [FR] [NL] [SP]
3. Access to public information
   - Assessment report
   - Model Policy Guidelines & Legislation texts [EN] [FR] [NL]
4. Privacy and data protection
   - Assessment report
   - Model Policy Guidelines & Legislation texts [EN] [FR] [NL] [SP]
5. Cybercrimes and cybersecurity
   - Assessment report
   - Model Policy Guidelines & Legislation texts [EN] [FR] [NL]
6. Interception of communications
   - Assessment report
   - Model Policy Guidelines & Legislation texts [EN] [FR] [NL]

II. Telecommunication acts:

Model Laws –Findings– ITU Models - HIPCAR

- Examples:
- “excess of a lawful excuse or justification”
- Illegal Remaining “remains logged in……or **continues to use** a computer system”
- SPAM “**initiates the transmission of multiple** electronic mail messages from or through such computer system” or “**materially falsifies header information** in multiple electronic mail messages and intentionally initiates the transmission of such messages”
- Data Espionage “computer data which are **not meant for him**”

Model Laws –Findings– ITU Models - HIPCAR

- 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**"

Model Laws –Findings– ITU Models - HIPCAR

- 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**"

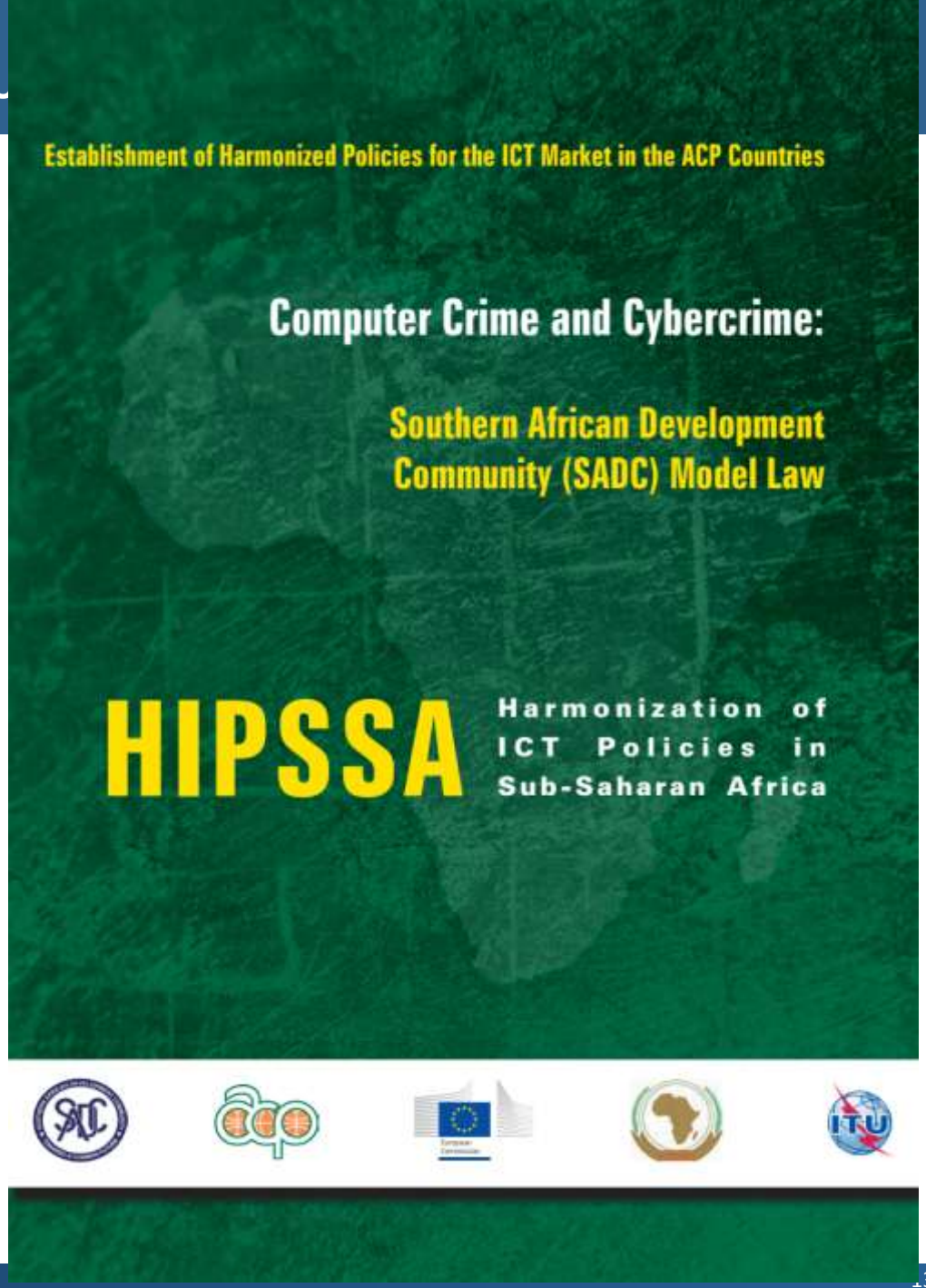
- is not liable for the information if

  a. 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

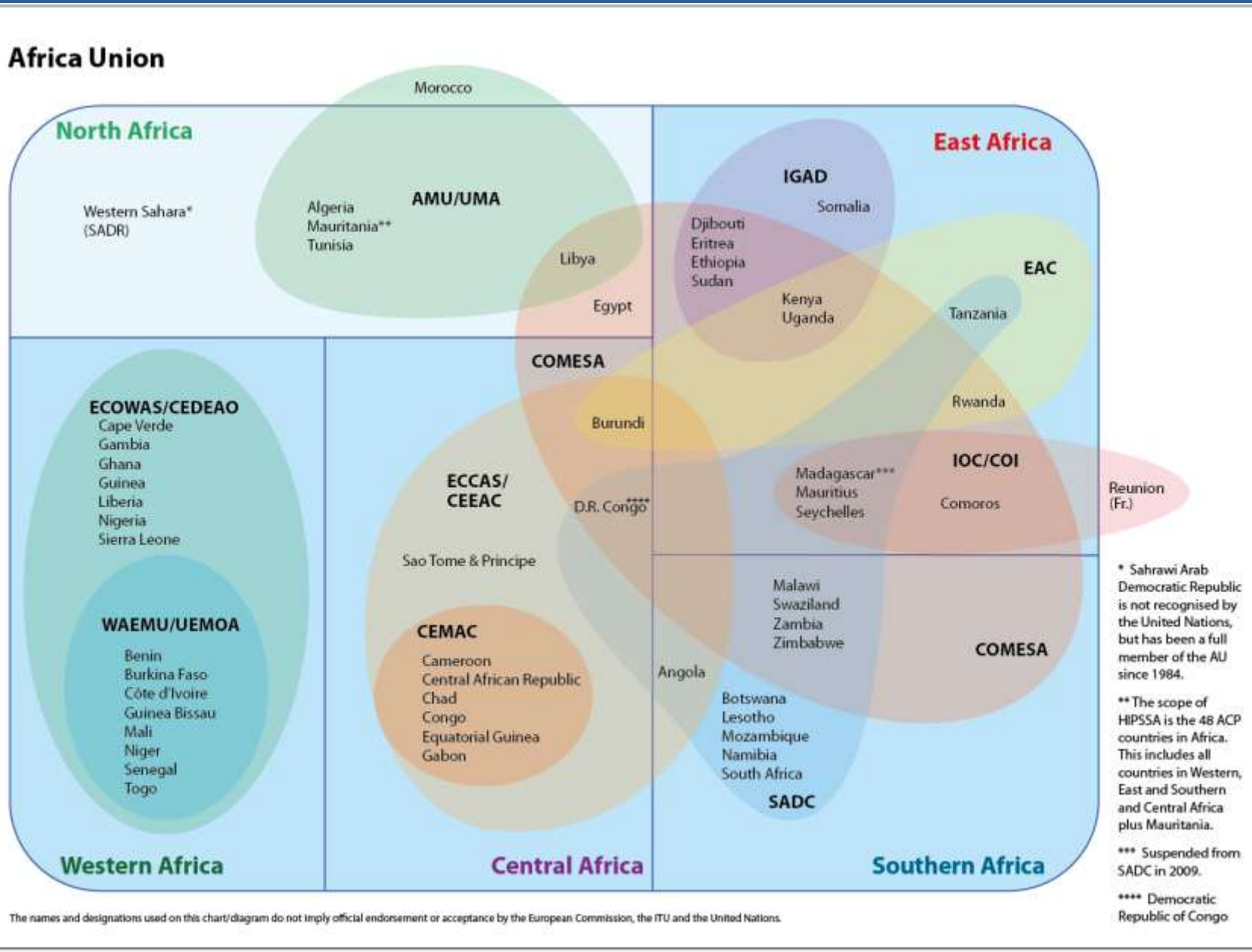
  b. the internet service provider, **upon obtaining knowledge or awareness** about **specific illegal information stored by other ways than an order from a public authority**, *expeditiously informs a public authority to enable them to evaluate the nature of the information and if necessary issue an order to remove the content.*

Model Laws –Findings– ITU

- ITU: HIPSSA



Model Laws –Findings– ITU Models - HIPSSA



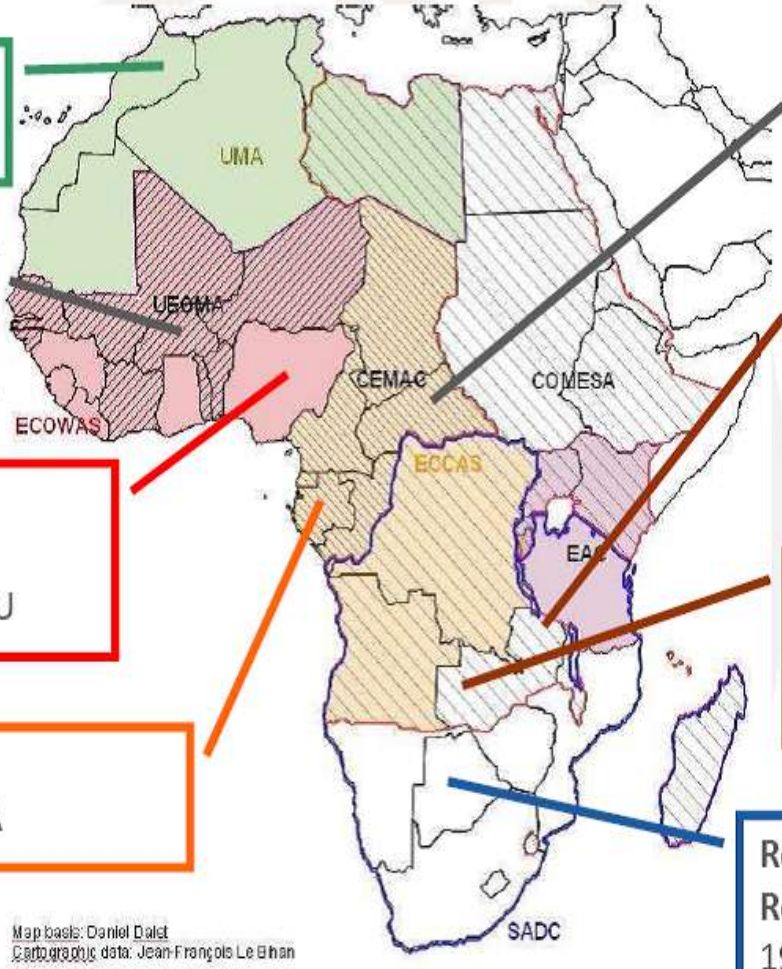
Model Laws –Findings– ITU Models - HIPSSA

UMA harmonization study
2010 funded by AfDB

UEMOA Directives
2004-2006

ECOWAS Supplementary Acts
ITU-EC Project
2005-2007 funded by EU and ITU

ECCAS reference framework
2007-2009 initiated with UNECA



CEMAC Directives
2007-2009 funded by OIF

Regional ICT Support Program (RICTSP)
2006-2009 funded by EU

Telecoms Harmonization
1998-2004 funded by USAID/REDSO

Regional Telecommunications Restructuring Program (RTRP)
1994-1998 funded by USAID

Model Laws –Findings– ITU Models - HIPSSA

3. Cross-border frequency coordination
   - HCM4A Sub-Saharan assessment report [EN] [FR]
   - HCM4A Central Africa assessment report [EN]
   - HCM4A East Africa assessment report [EN]
   - HCM4A Southern Africa assessment report [EN]
   - HCM4A West Africa assessment report [EN]
   - HCM4A Agreement [EN] [FR]
   - HCM4A Annexes to Agreement [Annex 1] [Annex 2A] [Annex 2B] [Annex 3A] [Annex 3B] [Annex 4] [Annex 5] [Annex 6] [Annex 6 App.1] [Annex 6 App.2] [Annex 6 App.3] [Annex 6 App.4] [Annex 6 App.5] [Annex 7] [Annex 8A] [Annex 8B] [Annex 9] [Annex 10] [Annex 11]

4. Regional ICT indicators
   - ICT-Eye website
   - Methodology [EN]

5. Interconnection cost-modeling
   - Assessment (regional and global)
   - Training materials [EN]
   - Training materials [FR]
   - Training materials [PT]

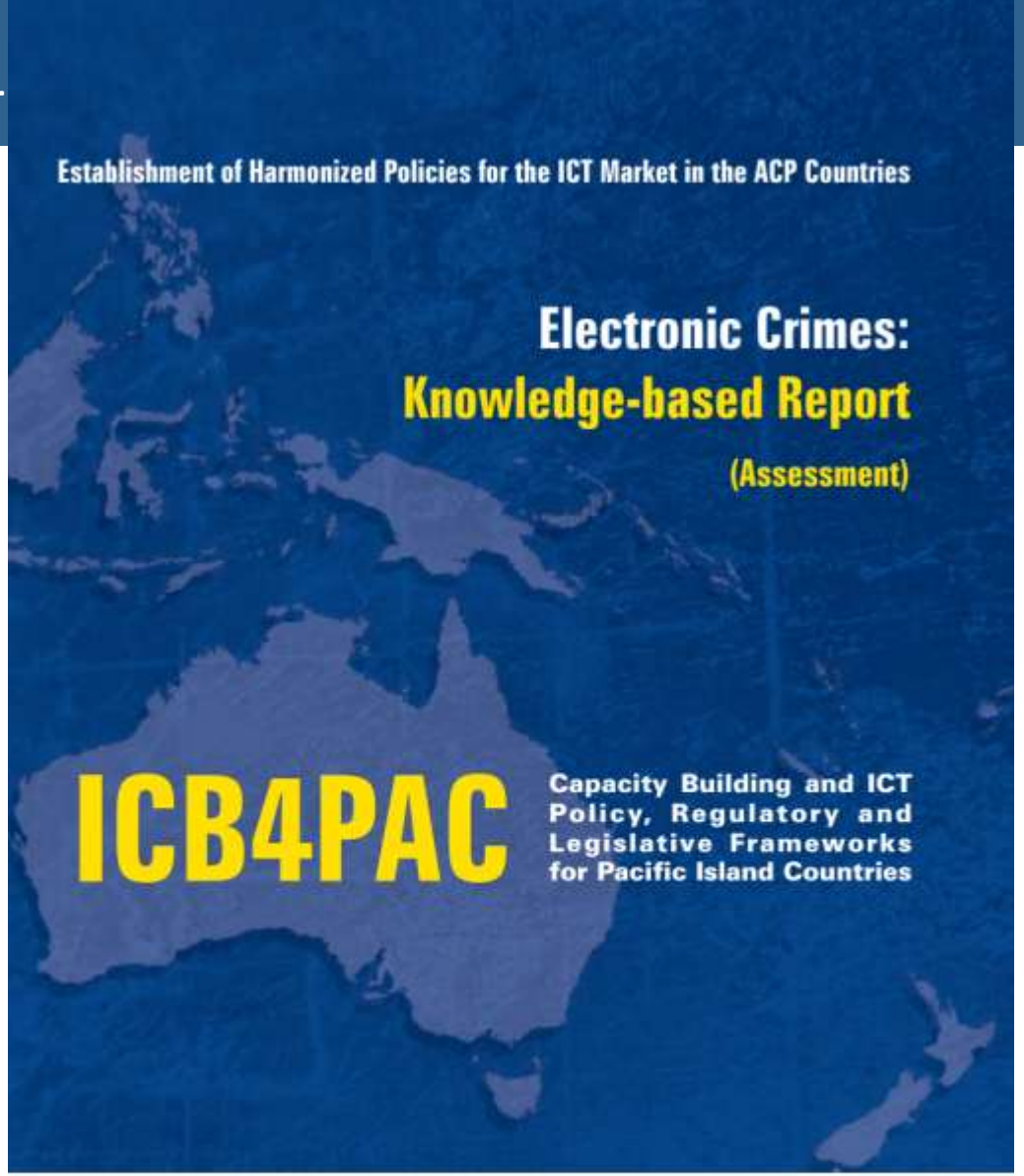
6. Cybersecurity
   - ECOWAS cybersecurity guidelines [EN]
   - ECCAS Model Law / CEMAC Directives on Cybersecurity (Data protection, e-transactions, cybercrime) [FR]
   - SADC model law on data protection [EN] [FR]
   - SADC model law on e-transactions [EN] [FR]
   - SADC model law on cybercrime [EN] [FR]

7. ICT/Telecom
   - ECCAS model law on ICT/Telecom [FR]

for ICT in ACP countries
Tel.: + 41 22 730 67 65
Fax.: + 41 22 730 54 84
E-mail: Sandro Bazzanella
International Telecommunication Union (ITU),
Telecommunication Development Bureau (BDT)
Place des Nations
CH-1211 Geneva 20
Switzerland

Model Laws –Findings–

- ITU: ICB4PAC



Model Laws –Findings– ITU Models – ICB4PAC

REGIONAL KNOWLEDGE-BASED REPORTS

1. Numbering
   - Knowledge-based report

2. National ICT Policy
   - Knowledge-based report

3. International Mobile Roaming
   - Knowledge-based report

4. Cybercrime
   - Knowledge-based report (Assessment)
   - Knowledge-based report (Skeleton)

5. Licensing
   - Knowledge-based report

6. Universal Access and Service
   - Knowledge-based report

7. Interconnection and Cost Modeling
   - Knowledge-based report

CONTACT INFORMATION

Mr. Sandro BAZZANELLA
Project Manager
ITU-EC Project-Harmonized Policies
for ICT in ACP countries
Tel.: + 41 22 730 67 65
Fax.: + 41 22 730 54 84
E-mail: Sandro Bazzanella
International Telecommunication Union (ITU),
Telecommunication Development Bureau
(BDT)
Place des Nations
CH-1211 Geneva 20
Switzerland

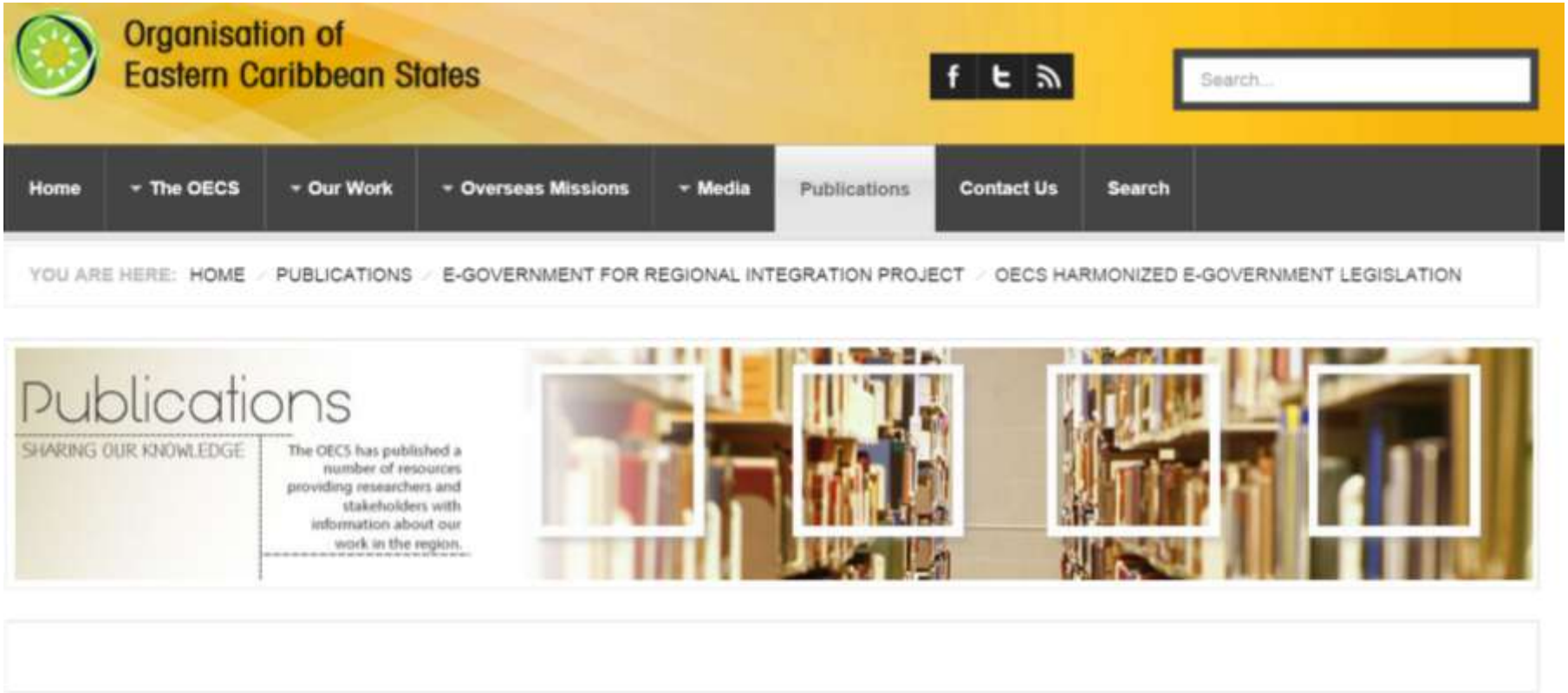
Model Laws –Findings– ITU Models – ICB4PAC

- HIPCAR Plus+

- ❑ "A country may criminalize racial and **religious acts** committed by using means of electronic systems"
- ❑ "A country may criminalize illegal online gambling"
- ❑ Cyber stalking "who initiates directly or **indirectly** any electronic communication, to do cyber stalking…….repeated coercion, intimidation, harassment, insult or **annoyance** through electronic……."
- ❑ "A country may criminalize defamation committed by means of electronic system"

Model Laws –Findings– World Bank/OECS – EGRIP Model

- World Bank/OECS – EGRIP:



Model Laws –Findings– World Bank/OECS – EGRIP Model

The suite of legislation includes:

- Electronic Transactions Act;
- Data Protection Act;
- Electronic Crimes Bill;
- Evidence Bill
- Electronic Funds Transfer Bill;
- EGRIP e-Filing Act;
- E-Filing Rules and Regulations

DOCUMENTS

Data Protection Act AGs 09.10.11 (docx, 97 KB) (75 downloads)	12 Feb 2014
Electronic Crimes Bill - AGs 09.10.11 (docx, 88 KB) (107 downloads) **Popular**	12 Feb 2014
Electronic Evidence Bill - AGs 09.10.11 (docx, 64 KB) (267 downloads) **Popular**	12 Feb 2014
Electronic Filing Bill AGs 09.10.11 (docx, 48 KB) (97 downloads)	12 Feb 2014
Electronic Filing Rules Regulations - AGs 09.10.11 (docx, 53 KB) (89 downloads)	12 Feb 2014
Electronic Funds Transfer Bill AGs 09.10.11 (docx, 60 KB) (86 downloads)	12 Feb 2014

Statistical Digest 2013-14

29 October 2014

- St Vincent & the Grenadines Education Statistical Digest 2013

  29 October 2014

- OECS Education Statistical Digest 2012-13

  29 October 2014

- Montserrat Statistical Digest 2013 2014

  29 October 2014

- Grenada Statistical Digest 2012 -3

  29 October 2014

- St Kitts and Nevis Statistical Digest 2014

  29 October 2014

REVISED TREATY ESTABLISHING TH UNION (PDF)

OECS Education St 13

EDUCA STRATE

Commu of the C

Model Laws –Findings– World Bank/OECS – EGRIP Model

ORGANISATION OF EASTERN CARIBBEAN STATES

Electronic Government for Regional Integration Project (EGRIP)

ELECTRONIC CRIMES BILL

Fourth Draft

6 October 2011

(With amendments from 20th Meeting of the OECS LAC)

Prepared by: Hellerstein & Associates

Model Laws –Findings– World Bank/OECS – EGRIP Model

- World Bank/OECS – EGRIP:

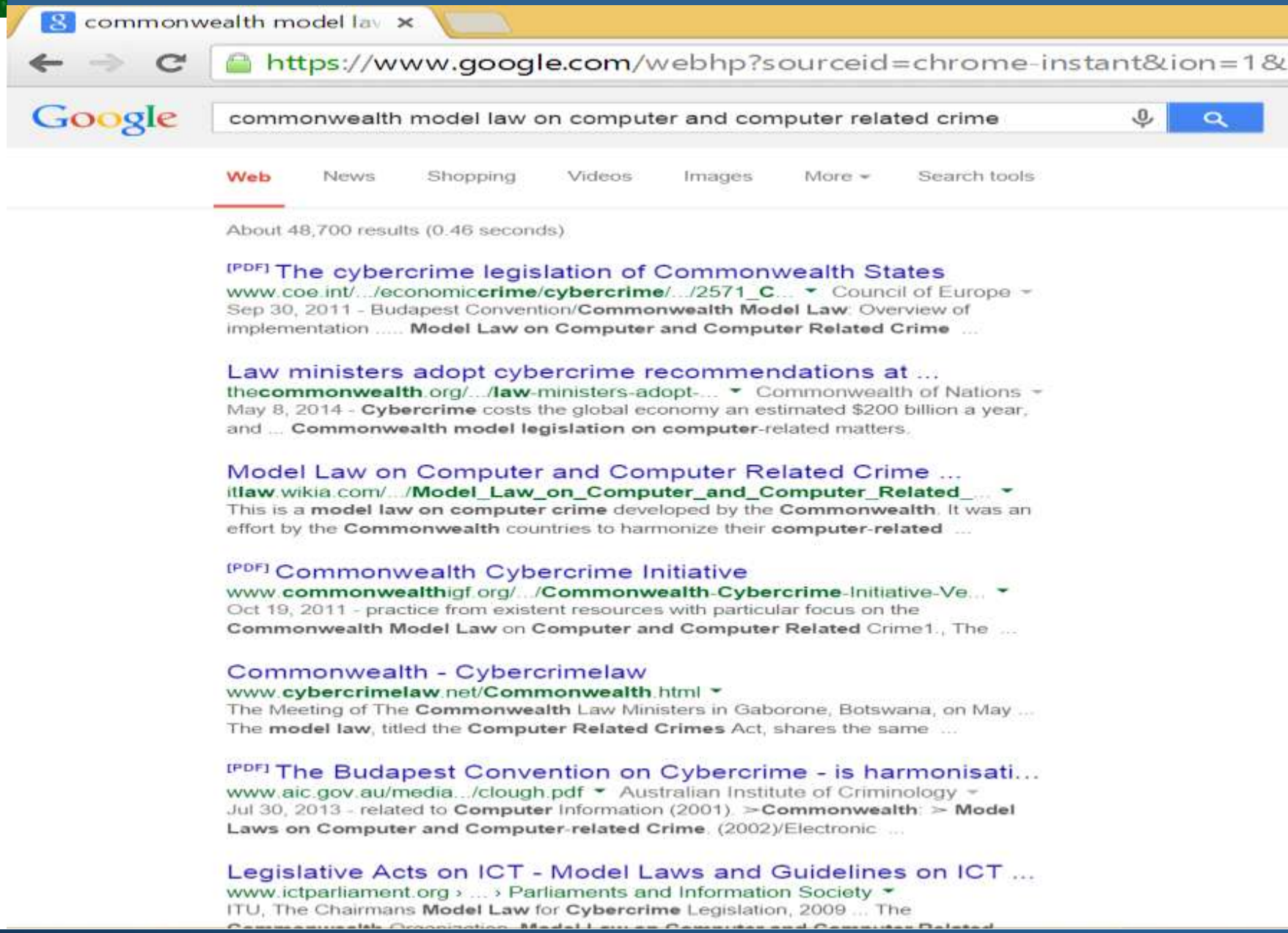
- ❑ Only one section on some aspects of illegal access & interference
- ❑ Rest not cybercrimes:
- ❑ Offensive messages and communications “inconvenience”
- ❑ Identity theft “not fraudulently or dishonestly make use of an **electronic signature, password** or other unique identification feature of another person”
- ❑ Defamation “person shall not defame another person….TBD”
- ❑ Malicious code “electronic program or a **hidden** function in a program that **infects data** with or without attaching its copy to a file and is **capable of spreading** over an electronic system with or without human intervention including virus, worm or Trojan horse”
- ❑ Violation of Privacy “captures, publishes or transmits the image of a **private area**…. naked or **undergarment clad genitals**, pubic area, **buttocks** or female breast”

Model Laws –Findings– World Bank/OECS – EGRIP Model

- World Bank/OECS – EGRIP:

- ❑ Prank calls to LEAs "use a caller ID service to transmit misleading or **inaccurate caller ID** information service"
- ❑ Electronic stalking "**embarrass**"
- ❑ Spoofing "establish a website or send an electronic message with a **counterfeit source**…with the intention that a visitor ….. believe ……authentic source……. to attract or solicit a person or electronic system"
- ❑ Unauthorized access to code "**not disclose**"
- ❑ Police obtain Court order to delete "**indecent** material"

Model Laws –Findings– Commonwealth Model Law



Model Laws –Findings– Commonwealth Model Law

The page cannot be found

The page you are looking for might have been removed, had its name changed, or is temporarily unavailable.

Please try the following:

- Make sure that the Web site address displayed in the address bar of your browser is spelled and formatted correctly.
- If you reached this page by clicking a link, contact the Web site administrator to alert them that the link is incorrectly formatted.
- Click the Back button to try another link.

HTTP Error 404 - File or directory not found.
Internet Information Services (IIS)

Technical Information (for support personnel)

- Go to Microsoft Product Support Services and perform a title search for the words **HTTP** and **404**.
- Open **IIS Help**, which is accessible in IIS Manager (inetmgr), and search for topics titled **Web Site Setup**, **Common Administrative Tasks**, and **About Custom Error Messages**.

Model Laws –Findings– Commonwealth Model Law

The Commonwealth

Page not found

The requested page "/shared_asp_files/uploadedfiles/%7bDA109CD2-5204-4FAB-AA77-86970A639B05%7d_Computer%20Crime.pdf" could not be found.

Model Laws –Findings– Commonwealth Model Law

The Commonwealth

Contacts \ Connects log-in \ Jobs \ Bookshop

Our work | Member countries | Newsroom | About us | Knowledge centre | Keyword search

Home > Search content

Content | Documents

Search content

With the exact phrase | With any of the words | Type

model law on computer | - Any - | Search

Search results for *model law on computer*

Communique: Commonwealth Law Ministers Meeting 2014

News item
8 May 2014
DRAFT **MODEL** LAW ON RECOGNITION AND ENFORCEMENT OF FOREIGN JUDGMENTS IN THE COMMONWEALTH 9. Ministers considered a draft **Model** ... the drafting of a **model** law as requested by Senior Officials at their 2010 ...

Law ministers adopt cybercrime recommendations at Botswana meeting

News item
8 May 2014
by using Commonwealth **model** legislation on computer-related matters. It also ...

Meeting of Law Ministers and Attorneys-General of Small Commonwealth Jurisdictions:

News item
12 September 2013
Draft **Model** Act on Integrity in Public Life ... jurisdictions asked the Secretariat to develop a **model** code of conduct for public ... and consultations were held and I am glad that a draft **model** Act is now before ...

Model Laws –Findings– Commonwealth Model Law

LMM(02)17

MODEL LAW ON COMPUTER AND COMPUTER RELATED CRIME

BACKGROUND

1. In Port of Spain, Law Ministers considered the impact of technology on various aspects of the law. One of the issues highlighted for further consideration was computer crime. Ministers recognized the challenges for law enforcement arising from the developments in technology including the new types of criminal activity and the difficulties associated with the gathering and use of electronic evidence. Ministers asked that an expert group be convened to consider the content of a model law on the basis of the work of the Council of Europe on the Draft Convention on Cyber Crime (*COE Draft Convention*). Topics that were specifically mentioned for consideration included criminalisation of various forms of computer abuse, admissibility of computer evidence, and investigation of computer related crime.

EXPERT GROUP

2. Following the course of action identified, the Secretariat convened an expert group to address the topic of Computer Crime and related issues.

3. Working on the basis of the *COE Draft Convention,* the expert group on Computer Crime and Related Criminal Law issues made recommendations, *inter alia*, for the content of a model law. On the basis of their report a draft model law, combined with the model law on e-commerce, was prepared and submitted to Senior Officials for their consideration.

SENIOR OFFICIALS

4. At their meeting in November 2001 Senior Officials decided that the Expert Group should be reconvened to review the draft model law in light of recent developments, in particular the changes made to the Council of Europe Convention on Cyber Crime, since the original meeting of the group. They also requested that the combined model law be separated into two model laws addressing the separate subject areas of e-commerce and computer crime and related issues.

5. The Expert Group was reconvened in March 2002 and based on their report (*Annex A*) a revised Model Law on Computer and Computer Related Crime was prepared. (*Annex B*).

6.
and c
chan

7. The Model Law on Computer and Computer Related Crime is recommended for endorsement by Law Ministers.

Model Laws –Findings– Commonwealth Model Law

- Not include:

  - ❑ E-forgery (Article 7 of the Convention)
  - ❑ E-fraud (Article 8)
  - ❑ Digital copyright/IPR protection (Article 10)
  - ❑ Corporate liability (Article 12)

Model Laws –Findings– Commonwealth Model Law

- 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
  - ❑ Adequate legislative language and procedural safeguards with respect to powers

  - ❑ International Cooperation provisions

Model Laws – Methodology

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

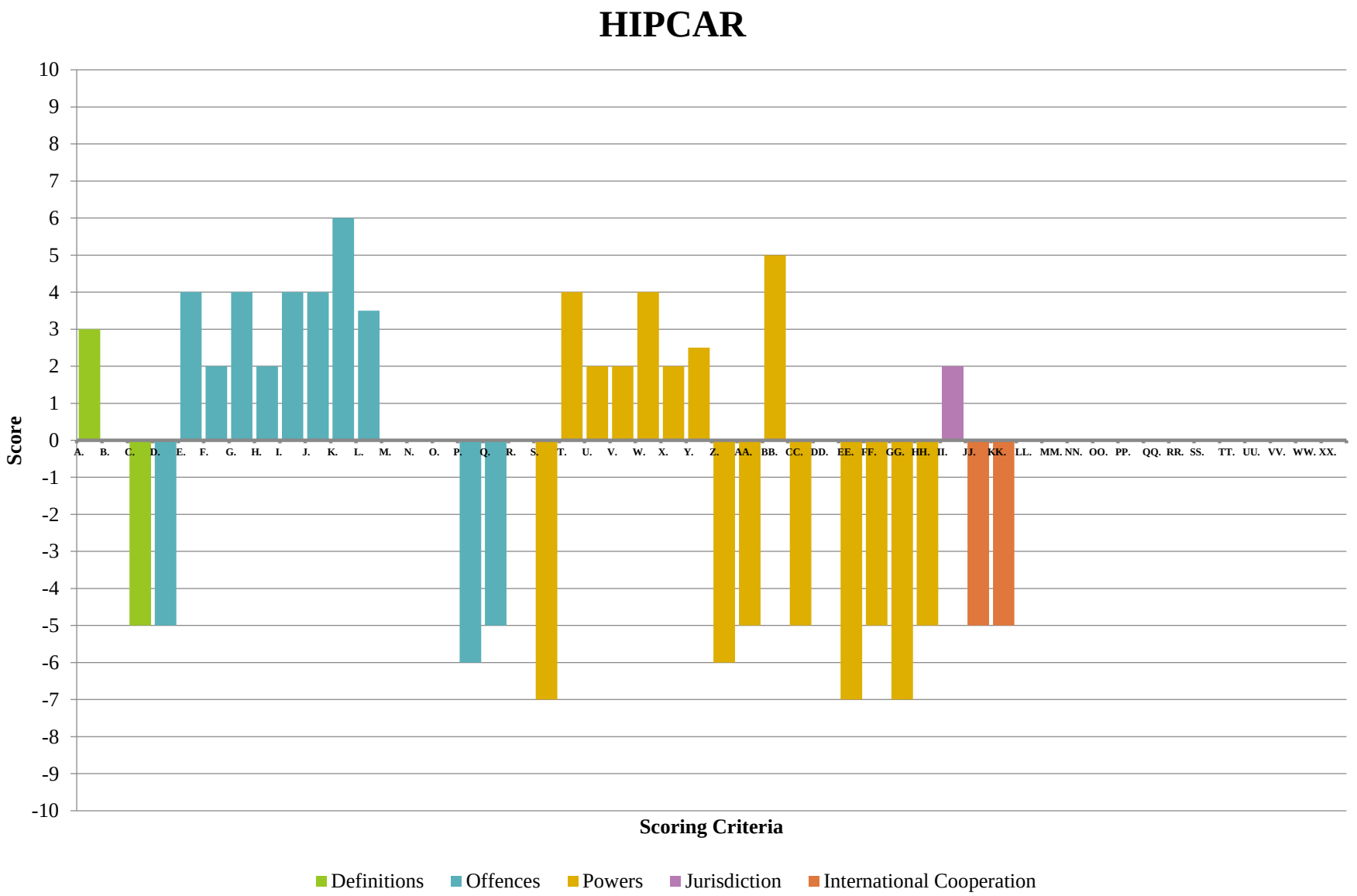
Model Laws – Methodology

	Section 2 – Procedural law	
R.	Applicability of procedural provisions to non-cyber offences	0
S.	Article 15 –Conditions and safeguards	-7
T.	Article 16 –Expedited preservation of stored computer data	4
U.	Article 17 –Expedited preservation and partial disclosure of traffic data	2
V.	Article 18 –Production order	2
W.	Article 19 –Search and seizure of stored computer data	4
X.	Article 20 –Real-time collection of traffic data	2
Y.	Article 21 –Interception of content data	2.5
Z.	Impact on Private Sector	-6
AA.	UNDHR/ ICCPR compliance	-5
BB.	Effective judicial supervision	5
CC.	Proportionality	-5
DD.	Grounds justifying application of powers	0
EE.	Limitation of scope and duration	-7
FF.	Privacy protection	-5
GG.	Consistency with international best practice on intermediary liability protection (OECD)	-7
HH.	Impact upon third parties	-5

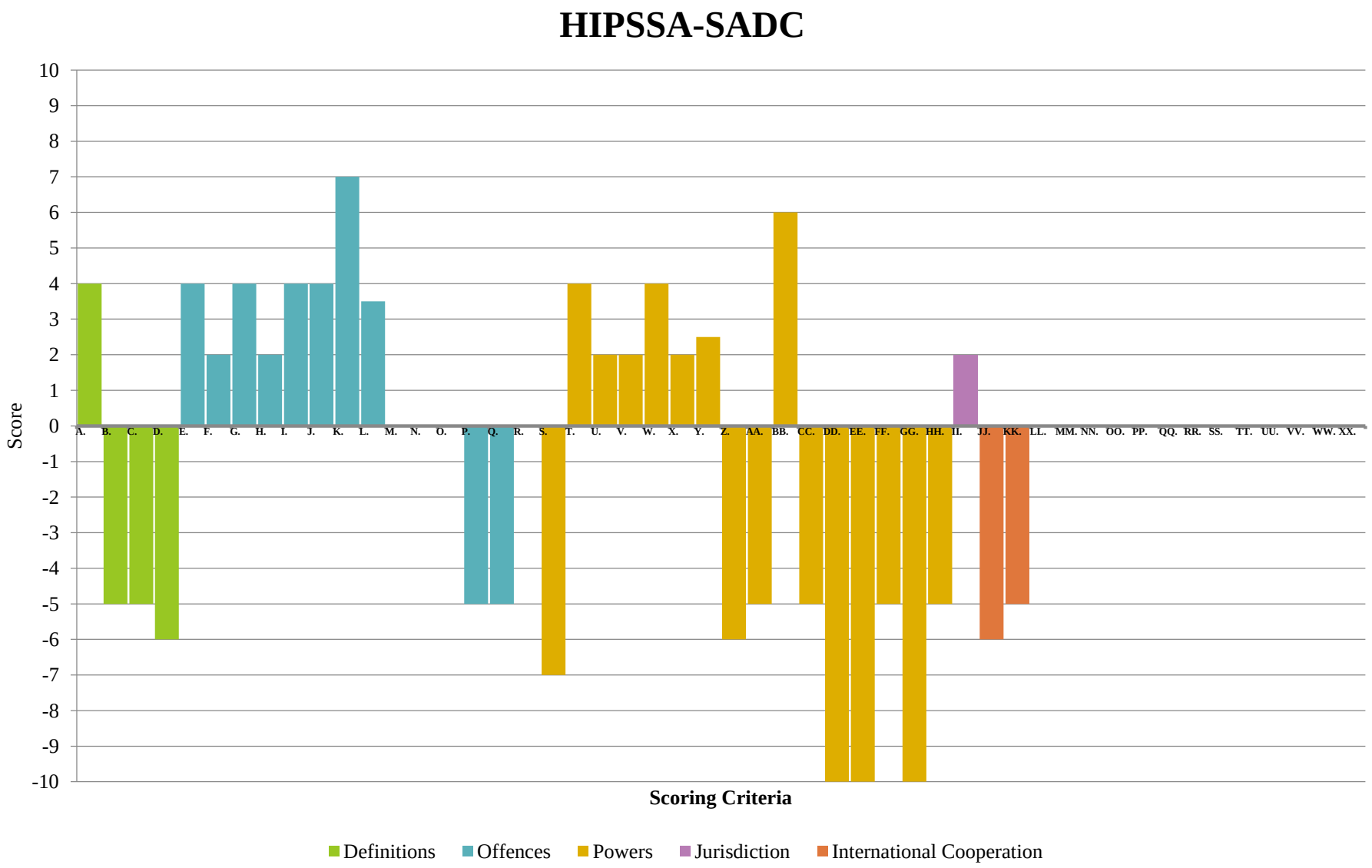
Model Laws – Methodology

II.	Article 22 –Jurisdiction	2
	Chapter III – International co-operation	
JJ.	Compatibility of offences for International Cooperation	-5
KK.	Compatibility of Powers for International Cooperation	-5
LL.	Article 23 –General principles relating to international co-operation	0
MM.	Article 24 –Extradition	0
NN.	Article 25 –General principles relating to mutual assistance	0
OO.	Article 26 –Spontaneous information	0
PP.	Article 27 –Procedures pertaining to mutual assistance requests in the absence of applicable international agreements	0
QQ.	Article 28 –Confidentiality and limitation on use	0
RR.	Article 29 –Expedited preservation of stored computer data	0
SS.	Article 30 –Expedited disclosure of preserved traffic data	0
TT.	Article 31 –Mutual assistance regarding accessing of stored computer data	0
UU.	Article 32 –Trans-border access to stored computer data with consent or where publicly available	0
VV.	Article 33 –Mutual assistance in the real-time collection of traffic data	0
WW.	Article 34 –Mutual assistance regarding the interception of content data	0
XX.	Article 35 –24/7 Network	0

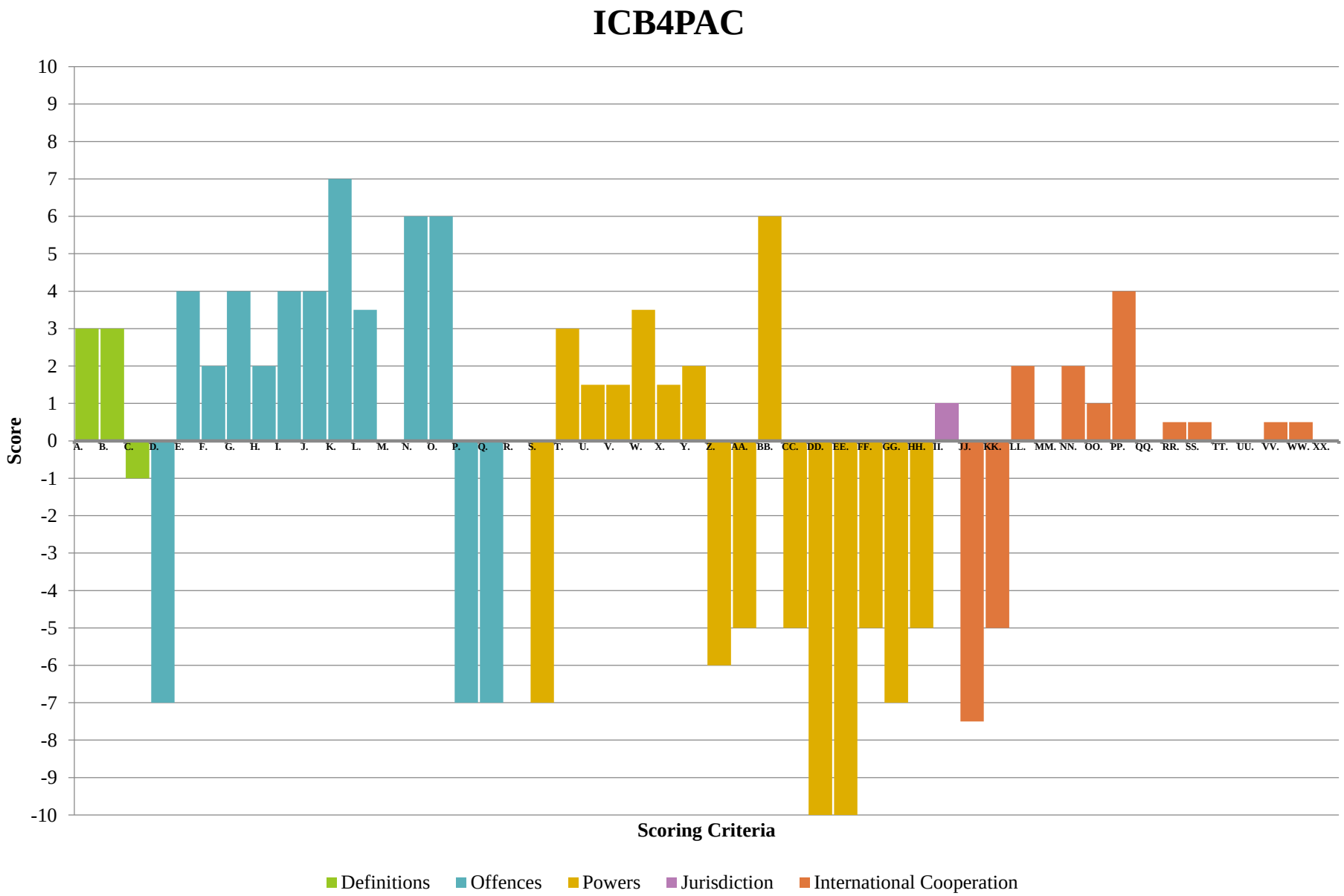
Model Laws –Findings– Methodology



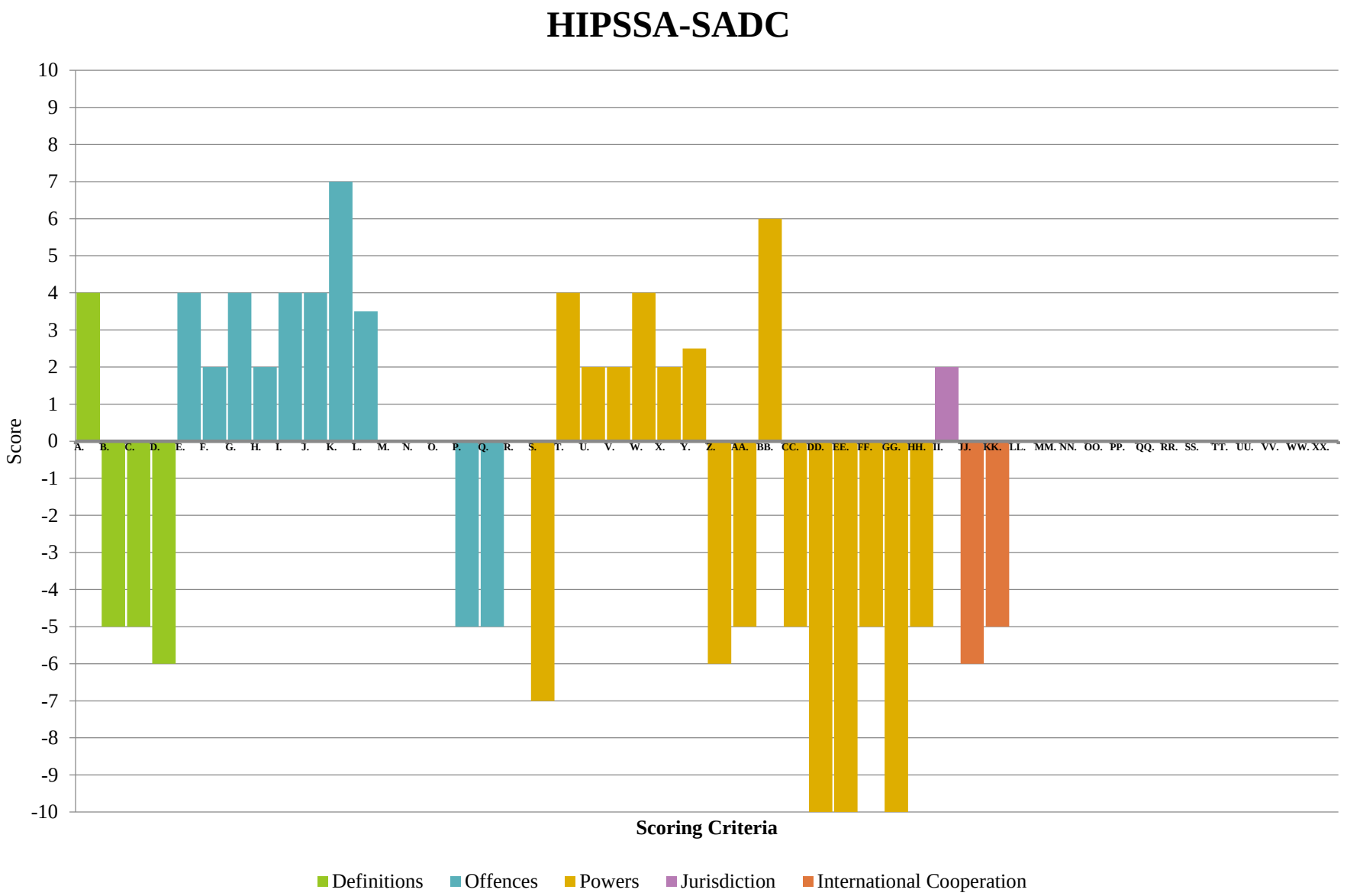
Model Laws –Findings– Methodology



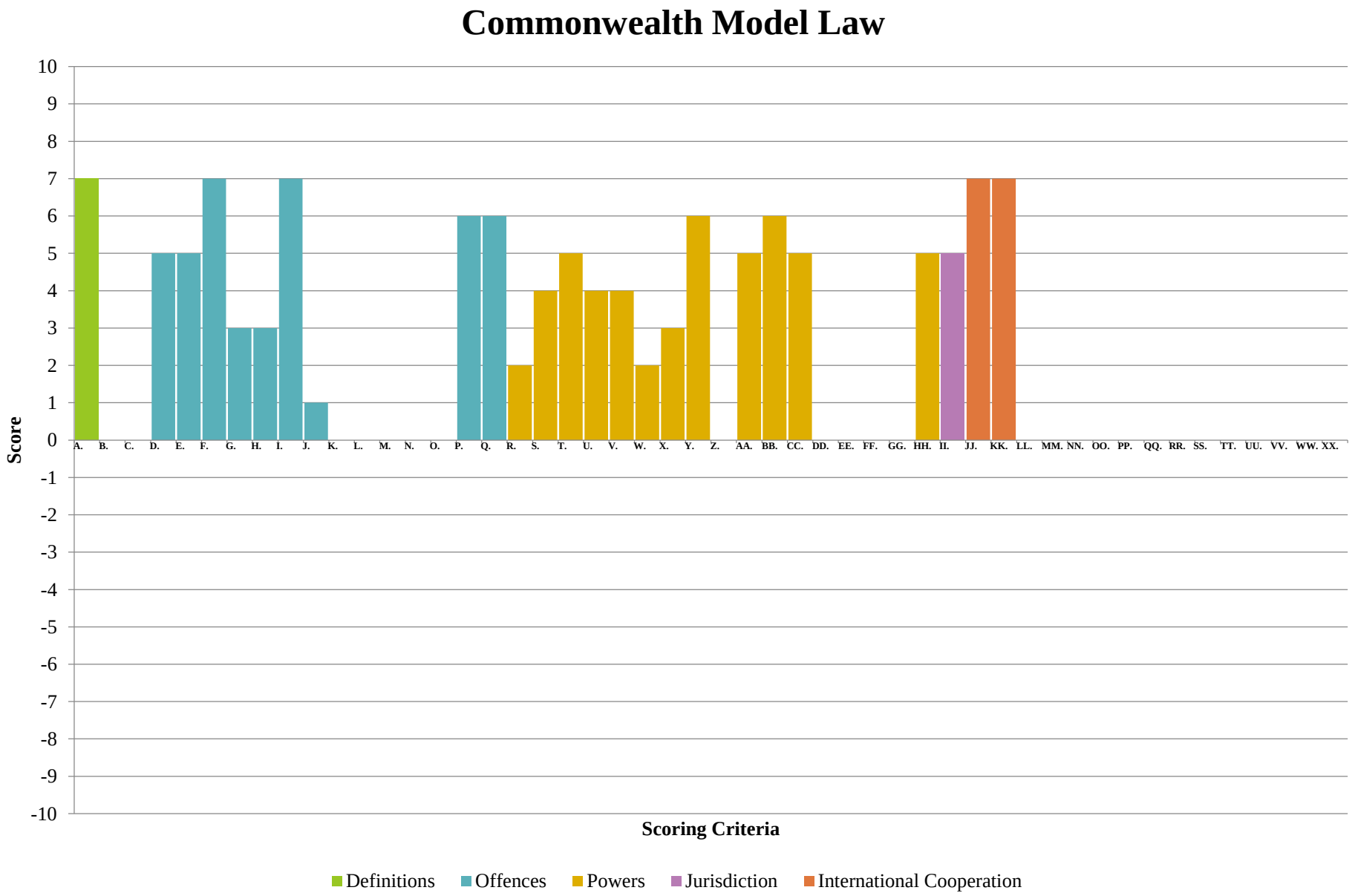
Model Laws –Findings– Methodology



Model Laws –Findings– Methodology



Model Laws –Findings– Methodology



Model Laws – Methodology

Model Laws – Conclusions

- Model Laws are:
  - ❑ Poor quality
  - ❑ Unsafe
  - ❑ Ambiguous (credibility)
  - ❑ Political agenda (at times - ITU)
  - ❑ Useful efforts sidelined (Commonwealth)
  - ❑ Utility doubtful

Model Laws – Conclusions

- Yet need:
  - ❑ Legislative Capacity Building
  - ❑ Convention + Eg. Implementation
  - ❑ Comprehendible, Accessible
  - ❑ Esp. for Developing Countries

Model Laws – Recommendations

- Break through Noise
  - ❑ Engagement with Countries not acceding/requesting accession on Legislative capacity building
- Mitigate, Contain
  - ❑ Engagement with Organizations on Model Laws
- Transparency
  - ❑ Seek clarification as to the status of model laws

Thank you!

Zahid Jamil, Esq.
Barrister
zahid@jamilandjamil.com