GLOBAL STATE of CYBERCRIME LEGISLATION

WEBINAR - MONDAY 27 APRIL 2020 11h00 FRANCE

www.coe.int/cybercrime

Speakers

- Alexander SEGER, Head of Cybercrime Division, Council of Europe
- Deborah WEISS, Permanent Secretary, Ministry of Communications, Fiji
- Momodou JALLOW, Principal ICT Officer, Ministry of Information and Communication Infrastructure, The Gambia
- Jayantha FERNANDO, Director/ Legal Advisor, ICT Agency of Sri Lanka

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

OBJECTIVE & EXPECTED OUTCOMES

To provide an overview of the global state of cybercrime legislation, illustrated by examples of reforms towards such legislation currently underway.

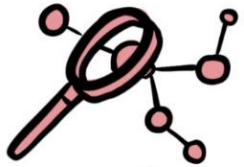
Participants will have a better understanding of

- progress made worldwide in recent years towards legislation on cybercrime and electronic evidence;
- why such legislation is particularly important to prosecute offenders that exploit the COVID-19 crisis to commit cybercrime;
- how to go about such reforms in their country and the type of support they can expect from the Cybercrime Programme Office of the Council of Europe to legislative reforms.

WHY LEGISLATION on CYBERCRIME & ELECTRONIC EVIDENCE?

Massive increase in cybercrime - Offences against & by means of computers

Cybercrime related to COVID-19 an illustration



Any crime may involve evidence on computer systems

Crime in cyberspace a threat to human rights, democracy and the rule of law

Effective criminal justice needed to ensure the rule of law in cyberspace

Response must be based on law and meet rule of law requirements

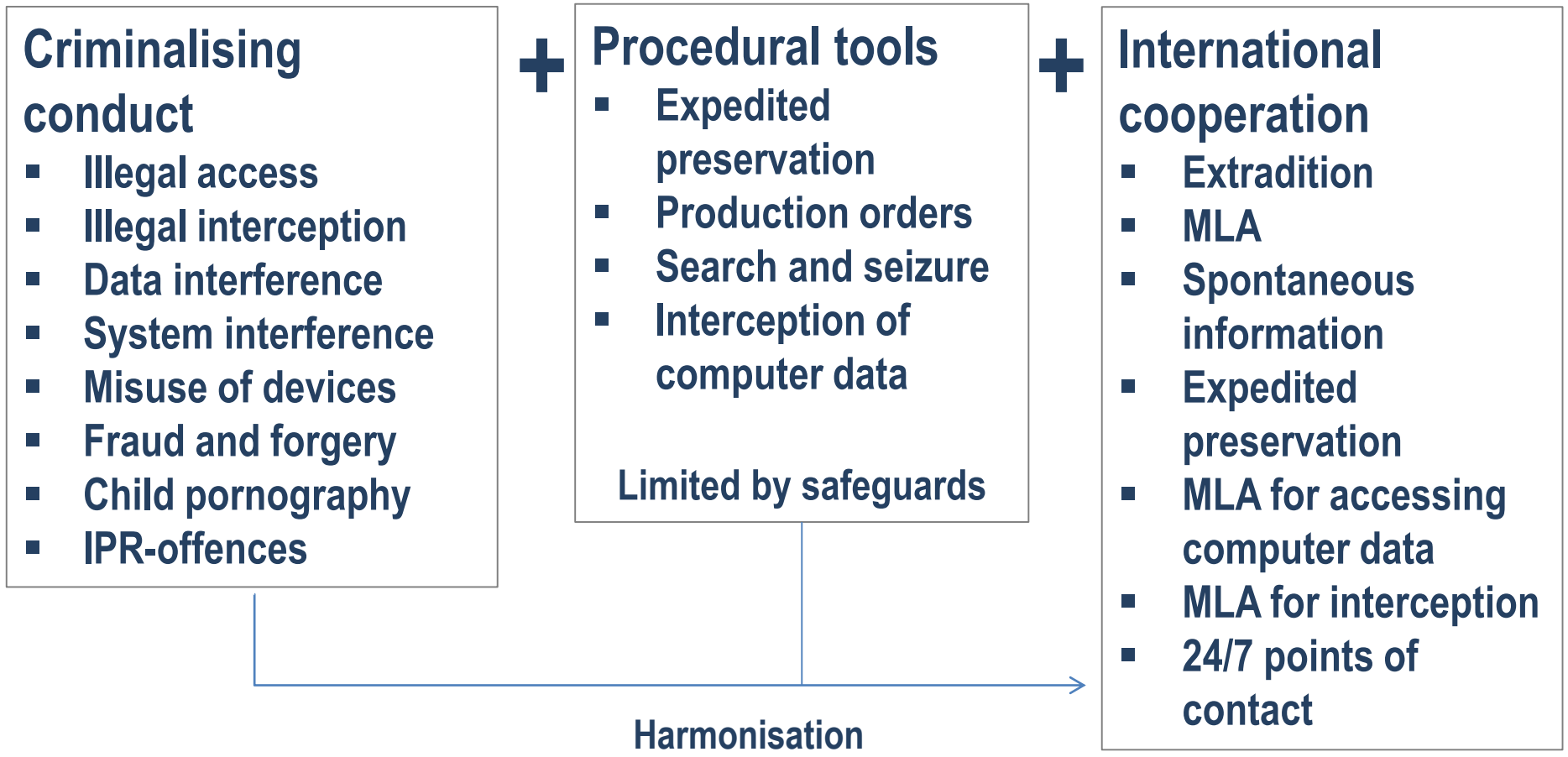
Establish offences in substantive criminal law

Provide law enforcement with powers to secure evidence on computer systems

Limit such powers by safeguards

Enable effective international cooperation

BUDAPEST CONVENTION: GLOBAL BENCHMARK for CYBERCRIME LEGISLATION



Procedural powers and international cooperation for any criminal offence involving evidence on a computer system!

THE CONVENTION COMPLEMENTED BY

1st Protocol on Xenophobia and Racism committed via Computer Systems (2003)

▶ 32 Parties + 12 Signatories

Guidance Notes on

- Notion of computer systems
- Botnets
- DDOS attacks
- Critical information infrastructure attacks
- Malware
- Spam
- ID theft
- Terrorism
- Transborder access to data (Article 32)
- Production Orders for Subscriber Information (Article 18)
- Election interference

2nd Protocol on enhanced international cooperation and access to evidence in the cloud

(currently under negotiation)

EXAMPLE: COVID 19 & CYBERCRIME

COVID-19 related crime in cyberspace

- Phishing campaigns and malware distribution through seemingly genuine information or advice on COVID-19 .
- Ransomware shutting down medical, scientific or other health-related facilities testing for COVID-19 or developing vaccines
- Ransomware targeting individuals through apps claiming to provide genuine information on COVID-19
- Attacks against critical infrastructures or international organizations
- Offenders targeting employees who are teleworking
- Fraud schemes offering personal protective equipment or fake medicines claiming to prevent or cure SARS-CoV-2
- Misinformation or fake news to create panic, social instability, xenophobia, racism or distrust in measures taken health authorities

Budapest Convention – Articles

- 2 – Illegal access
- 3 – Illegal interception
- 4 – Data interference
- 5 – System interference
- 6 – Misuse of devices
- 7 – Forgery
- 8 – Fraud
- 10 – IPR offences

Protocol on Xenophobia and Racism

Guidance Notes on

- Botnets
- DDOS attacks
- Critical information infrastructure attacks
- Malware
- Spam
- ID theft

Procedural powers to secure evidence and identify offenders

- 16+17 – Expedited preservation
- 18 – Production orders
- 19 – Search and seizure
- 20+21 – Interception

With safeguards

- Article 15

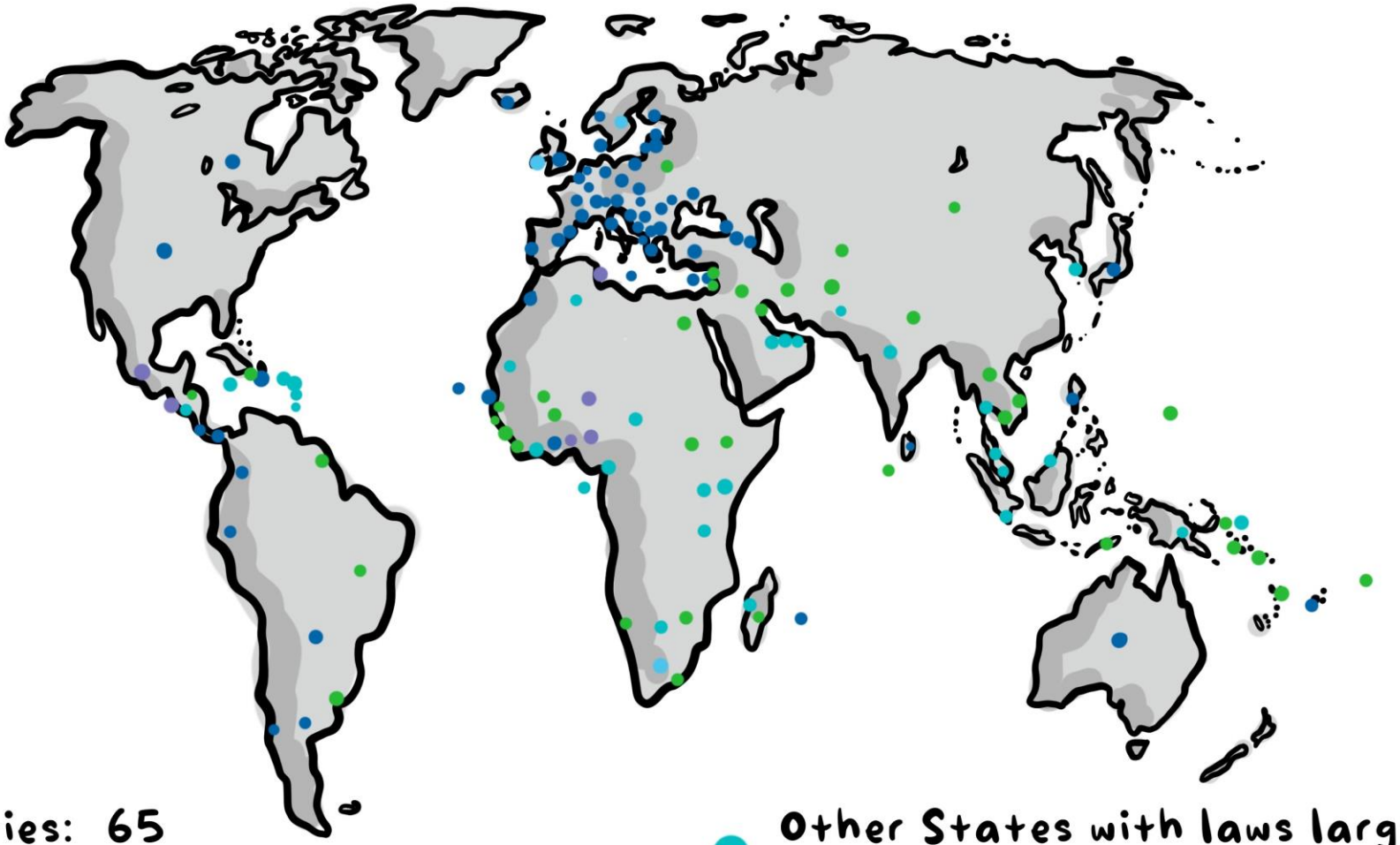
Guidance Note on

- Article 18 – Production orders

Framework for international cooperation

- Articles 23 - 35

REACH of the BUDAPEST CONVENTION



- Parties: 65
- Signed: 3
- Invited to accede: 8
  = 76+

- Other States with laws largely in line with Budapest Convention = 20+
- Further States drawing on Budapest Convention for legislation = 50+

GLOBAL STATE of CYBERCRIME LEGISLATION

The Council of Europe (through C-PROC) follows developments on legislation worldwide since 2013.

The latest update covers the Global State of Legislation as at February 2020

► Here is a summary of results!

GLOBAL STATE of CYBERCRIME LEGISLATION

Reforms of legislation on cybercrime and electronic evidence

		Underway or undertaken in recent years					
	States	By January 2013		By January 2018		By February 2020	
All Africa	54	25	46%	45	83%	46	85%
All Americas	35	25	71%	31	89%	32	91%
All Asia	42	34	81%	37	88%	38	90%
All Europe	48	47	98%	48	100%	48	100%
All Oceania	14	12	86%	12	86%	13	93%
All	193	143	74%	173	90%	177	92%

- By February 2020, 177 UN Member States (or 92%) were in the process of undertaking reforms of legislation on cybercrime and electronic evidence or had undertaken such reforms in recent years.
- The largest increase since 2013 has been noted in Africa.

GLOBAL STATE of CYBERCRIME LEGISLATION

Substantive criminal (offences against and by means of computer systems corresponding to Articles 2 to 10 Budapest Convention)

	States	Largely in place by January 2013		Largely in place by February 2020	
All Africa	54	6	11%	22	41%
All Americas	35	10	29%	17	49%
All Asia	42	13	31%	18	43%
All Europe	48	38	79%	44	92%
All Oceania	14	3	21%	5	36%
All	193	70	36%	106	55%

- By February 2020, 106 UN Member States (or 55%) had legislation in place with provisions criminalising offences against and by means of computers similar to those of the Budapest Convention.
- An increase of almost 20% since 2013.

GLOBAL STATE of CYBERCRIME LEGISLATION

Comment on substantive criminal law:

- ► Good practices available
- ► Concern: Laws on cybercrime used to prosecute speech

- The protection of national security and public order is a legitimate ground for restricting freedom of expression where that restriction is
  - prescribed by law
  - necessary in a democratic society
  - proportionate

- Broad, vaguely defined provisions do not meet these requirements
  - "use of computers with intent to compromise the independence of the state or its unity, integrity, safety or any of its high economic, political, social, military or security interests or subscribe, participate, negotiate, promote, contract or deal with an enemy in any way in order to destabilise security and public order or expose the country to danger …"
  - "use of computers to create chaos in order to weaken the trust of the electronic system of the state or provoke or promote armed disobedience, provoke religious or sectarian strife, disturb public order, or harm the reputation of the country … "
  - "creation of sites with a view to disseminating ideas contrary to public order or morality"

- Problematic trend ► Discredits legitimate action on cybercrime ► violates fundamental rights

GLOBAL STATE of CYBERCRIME LEGISLATION

Specific procedural powers to secure e-evidence

		Procedural legislation largely in place					
	States	By January 2013		By January 2018		By February 2020	
All Africa	54	5	9%	10	19%	16	30%
All Americas	35	5	14%	9	26%	12	34%
All Asia	42	8	19%	13	31%	11	26%
All Europe	48	31	65%	39	81%	39	81%
All Oceania	14	1	7%	3	21%	4	29%
All	193	50	26%	74	38%	82	42%

- By February 2020, 82 UN Member States (or 42%) had legislation in place with specific provisions to secure electronic evidence on computer systems in relation to any crime.
- An increase of 16% since 2013 but more progress is needed.

Comment on procedural powers to secure electronic evidence

- Good practices available
- Increasing data protection regulations (Data Protection Convention 108 ► Cabo Verde, Mauritius, Morocco, Senegal + reforms in others)

- Often reliance on general powers
- Problem of safeguards

Links to the Budapest Convention

		Party, signatory or invited to accede					
States		By January 2013		By January 2018		By February 2020	
All Africa	54	3	6%	8	15%	10	19%
All Americas	35	8	23%	11	31%	12	34%
All Asia	42	2	5%	4	10%	4	10%
All Europe	48	43	90%	46	96%	46	96%
All Oceania	14	1	7%	2	14%	2	14%
All	193	57	30%	71	37%	74	38%

Update April 2020: + Guatemala + Niger invited to accede

- Steady progress in membership in the Budapest Convention

Links to the Budapest Convention

		Use of Budapest Convention as guideline or source					
States		By January 2013		By January 2018		By February 2020	
All Africa	54	21	39%	33	61%	38	70%
All Americas	35	22	63%	24	69%	26	74%
All Asia	42	25	60%	27	64%	28	67%
All Europe	48	46	96%	47	98%	47	98%
All Oceania	14	10	71%	11	79%	14	100%
All	193	124	64%	142	74%	153	79%

- Global impact of the Budapest Convention in terms of legislation
  ► a guideline or source of inspiration for domestic legislation in 153 States (or 79%)

GLOBAL STATE of CYBERCRIME LEGISLATION : CONCLUSIONS

CRIMINALISING ATTACKS AGAINST AND BY MEANS OF COMPUTERS

✓ Good progress

? Some concerns over vague, broadly defined provisions

PROCEDURAL POWERS TO SECURE ELECTRONIC EVIDENCE

✓ Progress in many countries

✓ Progress in terms of data protection regulations

? Specific, well-defined powers with conditions and safeguards still needed in a number of countries

BUDAPEST CONVENTION ON CYBERCRIME IS RELEVANT WORLDWIDE

✓ Used as guideline in an increasing number of countries

✓ Some countries have joined or are joining to benefit from membership

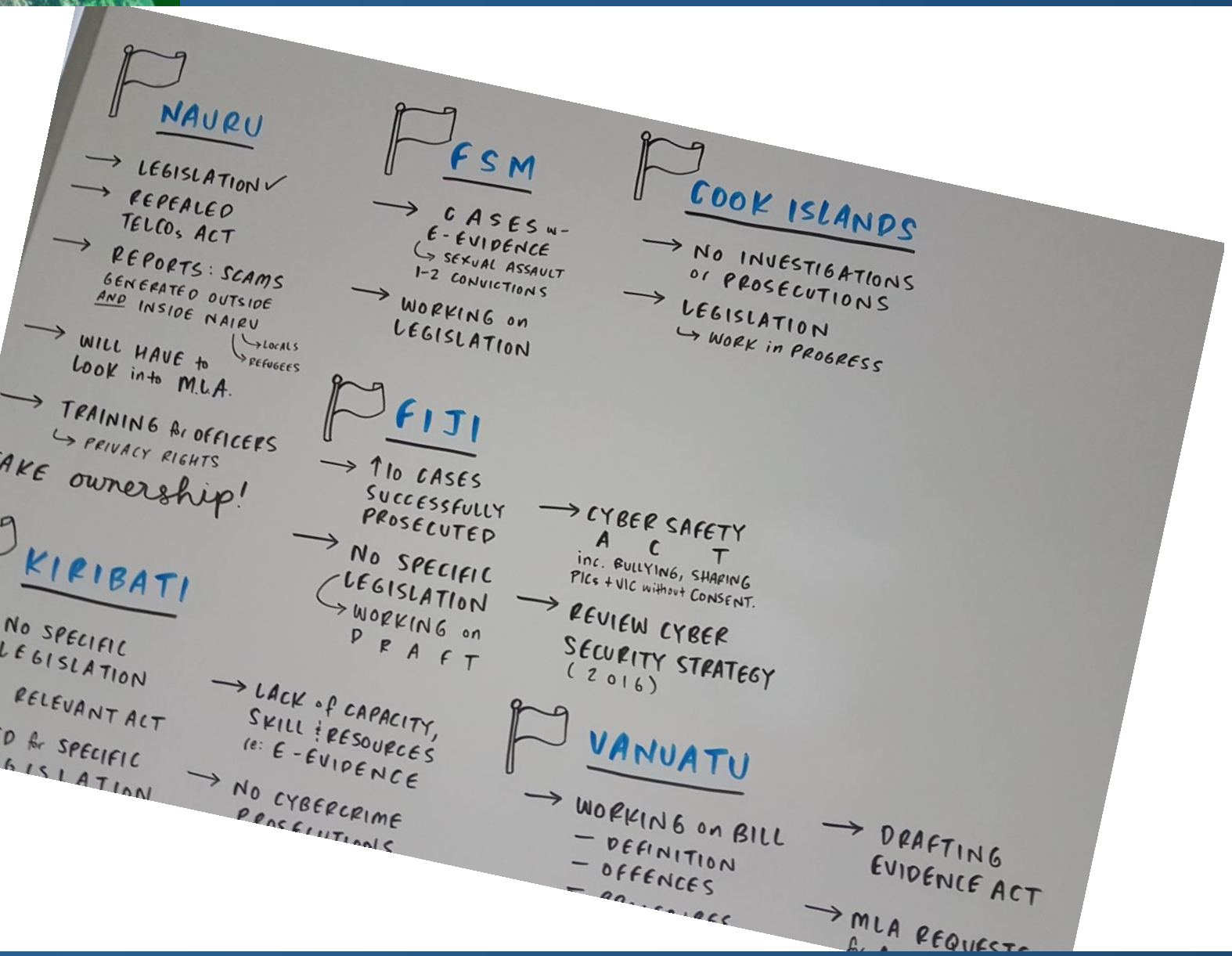
LEGISLATION MUST BE BACKED UP BY CAPACITY BUILDING

The Cybercrime Programme Office of the Council of Europe (C-PROC) is ready to support you!

GLOBAL STATE of CYBERCRIME LEGISLATION : CONCLUSIONS

ANY QUESTIONS?

REFORM of CYBERCRIME LEGISLATION: FIJI



Deborah WEISS,
Permanent Secretary,
Ministry of Communications,
Fiji

REFORM of CYBERCRIME LEGISLATION: FIJI

Deborah WEISS,
Permanent Secretary,
Ministry of Communications,
Fiji

Cybercrime Legislation in The Gambia

Momodou Alieu Jallow - Principal ICT Officer
Ministry of Information and Communication Infrastructure
The Gambia

Content

- Background and Some data on ICTs
- Cybercrime Legislation So far
  - The Gambia Cybercrime Bill 2020
- Plans ahead

Background of The Gambia

ICT Ecosystem

- 6 licensed Internet Service Providers
- 4 GSM operators

ICT Ecosystem Cont.

- Internet Penetration Rate is at 70%
- Mobile penetration rate is at 147%
- The Gambia is connected to the rest of the world through the ACE cable with over 100GB capacity
- Has a total land area of 10, 000 sq.km. with about 1300 Km of fiber as national backbone

Laws of The Gambia

- The Gambia uses the common law system
- Cybercrime prosecution has not been very effective in the Gambia because of lack enough procedural powers and responsive international cooperation
- Part III of Chapter III of the existing ICT Act 2009 is related to Computer Misuse and Cyber Crime. Part IV of the same chapter relates to the protection of children.
- Part V of Chapter III of the existing IC ACT 2009 introduces provisions on procedural elements, mainly related to the retention of information (Art. 181-Art.182). The legislative text doesn't propose provisions on electronic evidence. However Part V of Chapter III introduces the notion of electronic records and their use. The definition of record is not given by the text.

Cybercrime Legislation So far

- having had the National Cybersecurity Strategy and Action Plan in 2016, it has been an objective / outcome to get a comprehensive cybercrime bill
- In 2017 The Gambia started engagement with the Council of Europe,
- In May 2018, an advisory mission was sent by COE that assessed the laws of the Gambia and relevant gaps identified in our various laws; capacity building workshop
- In March 2019, COE sent a delegation, a 3-days workshop was held that drafted the cybercrime bill. Commonwealth also took part in the drafting workshop.

Cybercrime Legislation So far cont.

- In February 2020, the cybercrime bill was validated.
- Currently the bill is with cabinet for consideration!!!

The Gambia Cybercrime Bill 2020

Part I – Preliminary

Part II – Offences

Part – III Procedural measures

Part IV – International co-operation

Part V – Miscellaneous provisions

The Gambia Cybercrime Bill 2020 Cont.

Part II – Offences

- Unauthorised access to computer data
- Unauthorised interception of computer data
- Unauthorised acts in relation to a computer system or data
- Unauthorised supply or possession of computer systems or other device, or computer data
- Computer related extortion, fraud and forgery
- Child Pornography
- Offences related to infringements of copyright and related rights – adopted the provisions of the Copy Right Law
- Attempt, aiding or abetting
- Criminal liability of legal entities
- Sanction or measures

The Gambia Cybercrime Bill 2020 Cont.

Part - III Procedural measures

- Search and seizure of stored computer data
- Real-time collection of traffic data
- Interception of content data
- Expedited preservation of stored computer data
- Expedited preservation and partial disclosure of traffic data
- Production order

The Gambia Cybercrime Bill 2020 Cont.

Part IV - International co-operation

- General principles relating to international co-operation
- Extradition
- General principles relating to mutual assistance
- Spontaneous information
- Confidentiality and limitation on use
- 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 with consent or where publicly available
- Mutual assistance regarding the real-time collection of traffic data
- Mutual assistance regarding the interception of content data
- 24/7 network

Plans ahead

- An engagement workshop with the National Assembly Select Committee on ICT
- Series of capacity building activities
- Data Protection and Privacy Legislation formulation
- IC Act 2009 Review; cybersecurity laws for the protection of NCI and NCII
- GMCSIRT is being established with the regulator PURA.

THANK YOU

ANY QUESTIONS?

Reform of cybercrime legislation in Asia: Comments

Jayantha FERNANDO
Director/ Legal Advisor
ICT Agency of Sri Lanka

ANY QUESTIONS?