EUROMED JUSTICE

A programme funded by the European Union

EUROMED JUSTICE

Legal and Gaps Analysis
Cybercrime

CrimEx
EuroMed Justice Group of Experts in Criminal Matters

ALGERIA, EGYPT, ISRAEL, JORDAN, LEBANON, MOROCCO, PALESTINE, TUNISIA

EuroMed Justice Expert: Mr Daniel Suter, UK

Lead Firm /Chef de file

FIIAPP COOPERACIÓN ESPAÑOLA

EIPA

CILC Center for International Legal Cooperation

Justice Coopération Internationale

AUTHOR(S):

This Legal and Gaps Analysis has been written by Mr. David Mayor Fernandez (Spain), in collaboration with: Mr. Dan Suter (Director iJust International - United Kingdom), Mr. Giel Franssen (The Netherlands), and Professor Dr. Mohamed Elewa Badar (Egypt- United Kingdom).

EDITOR AND COORDINATOR:

Virgil Ivan-Cucu, EuroMed Justice Key Expert, Senior Lecturer EIPA Luxembourg.

LINGUISTIC VERSIONS

Original: EN
Manuscript completed in November 2017.

DISCLAIMER

The information contained in this Legal and Gaps Analysis is based on the research and data provided by the senior experts assigned, and the representatives of the Southern Partners Countries in the framework of the work carried out under the EuroMed Justice Project, except for Lebanon. In conformity with Lebanese Law none of the Lebanese judges and representatives contributed to the work in any mean or way. The Consortium implementing this EuroMed Justice project cannot be held responsible for the accuracy, actuality or exhaustiveness of the analysis, nor can it be made liable for any errors or omissions, contained in this document.

This publication has been produced with the assistance of the European Commission. The contents of this publication can in no way be taken to reflect the views of the European Commission.

COPYRIGHT

www.euromed-justice.eu

Contents

ABBREVIATIONS 5

GLOSSARY 6

INTRODUCTION 12
Cybercrime in the Southern Partner Countries 12
Cyber Threats 13
International Dimensions 14

METHODOLOGY 15
Legal Analysis........ 15
Gap Analysis........ 16

CONTEXT 17
International Approaches........ 17
United Nations 17
Council of Europe........ 18
African Union 19
Arab League........ 19
Harmonization of ICT Policies, Legislation and Regulatory Procedure........ 20
International Centre for Missing and Exploited Children........ 21

LEGAL AND GAP ANALYSES........ 22
Algeria........ 22
Offences 22
Procedure........ 45
International Cooperation 60
Egypt 74
Offences 74
Procedure........ 97
International Cooperation 115
Israel 130
Offences 130
Procedure........ 143
International Cooperation 153
Jordan 158
Offences 158
Procedure........ 177
International Cooperation 194
Lebanon 208
Offences 208
Procedure........ 232

International Cooperation 249
Morocco 264
Offences 264
Procedure 287
International Cooperation 306
Palestine 320
Offences 320
Procedure 344
International Cooperation 351
Tunisia 361
Offences 361
Procedure 385
International Cooperation 403

CONCLUSION 418

ANNEX A 419

Abbreviations

AU	African Union
AUC	African Union Convention on Cyber Security and Personal Data Protection
BC	Budapest Convention on Cybercrime of the Council of Europe
BSI	Basic Subscriber Information
CA	Central Authority
CERT	Cyber Event Readiness Team
CITO	Arab League Convention on Combating Information Technology Offences
CTED	United Nations Counter-Terrorism Executive Directorate
DDoS	Distributed Denial of Service
CSPs	Communication Service Providers
HIPCAR	Harmonization of ICT Policies, Legislation and Regulatory Procedure
IAP	International Association of Prosecutors
ICMEC	International Centre for Missing and Exploited Children
ICT	Information and Communication Technologies
INTERPOL	The International Police Organization
ITU	International Telecommunications Union
LoRs	Letters of Request
MLA	Mutual Legal Assistance
MMS	Multimedia Messaging Service
MOU	Memorandum of Understanding
PA	Palestinian Authority
SMS	Short Message Service
SPC	Southern Partner Country
TRIPS	The Agreement on Trade-Related Aspects of Intellectual Property Rights
UNTOC	United Nations Convention Against Transnational Organized Crime
URL	Uniform Resource Locator
UNODC	United Nations Office on Drugs and Crime

Glossary

Basic Subscriber Information (BSI)

BSI may be contained in the form of computer data or any other form, such as paper records and includes information that describes who a person is (e.g., the name and address of the subscriber/account holder), and may include details about the person's use of an online service on a specific date and time (for example, times of logging into the account, how long the subscriber has used that specific service, etc.). ''Subscriber'' is intended to include a broad range of service provider clients, from persons holding paid subscriptions, to those paying on a per-use basis, to those receiving free services. It also includes information concerning persons entitled to use the subscriber's account.[1]

Botnet

A network of computers that have been infected by malicious software (computer virus). Such a network of compromised computers ('zombies') may be activated to perform specific actions, such as attacking information systems (cyber attacks). These 'zombies' can be controlled – often without the knowledge of the users of the compromised computers – by another computer. This 'controlling' computer is also known as the 'command-and-control centre'[2]

Communications Service Provider (CSP)

A communications service provider transports information electronically, and encompasses companies in the telecom (landline and wireless), internet, cable, satellite, and social media services.

Computer system

Any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data[3]

[1] Explanatory Report Budapest Convention paragraph 177

[2] T-CY Guidance Notes – 1 March 2017 p 6

[3] Article 1.a. Budapest Convention

Cryptocurrency

A digital asset designed to work as a medium of exchange using cryptography to secure the transactions and to control the creation of additional units of the currency[4]

Cyberbullying or cyberharassment

Bullying or harassment using electronic forms of contact that has become increasingly common, especially among teenagers

Dark web

The dark web forms a small part of the deep web, the part of the world wide web not indexed by search engines.[5]

Distributed Denial of Service

Denial of service (DOS) attacks are attempts to render a computer system unavailable to users through a variety of means. These may include saturating the target computers or networks with external communication requests, thereby hindering service to legitimate users. Distributed denial of service (DDOS) attacks are denial of service attacks executed by many computers at the same time. There are currently a number of common ways by which DOS and DDOS attacks may be conducted. They include, for example, sending malformed queries to a computer system; exceeding the capacity limit for users; and sending more e-mails to e-mail servers than the system can receive and handle[6]

Dual Criminality

This requires that the particular acts alleged are a crime in the requested and the requesting State. The elements of the analogous offences need not be the same, but they must be sufficiently familiar that the conduct is criminal in both states.

[4] Andy Greenberg (20 April 2011) Crypto Currency

[5] Andy Greenberg (19 November 2014) Hacker Lexicon: What is the dark web?

[6] T-CY Guidance Notes – 1 March 2017 p 18

Encryption

Is the process of encoding a message or information in such a way that only authorized parties can access it (also see end-to-end encryption below)

End-to-end encryption

End-to-end encryption (E2EE) is a system of communication where only the communicating users can read the messages. E2EE is designed to defeat any attempts at surveillance or tampering because no third parties can decipher the data being communicated or stored in servers. For example, companies, such as WhatsApp, that use end-to-end encryption are unable to hand over texts of their customers' messages to law enforcement.

Hacking

The breach of security defences to gain illegal access into a computer system.

Hacktavist

A hacker who subversively uses computers and computer networks to promote a political agenda or social change.

IP Address

An Internet Protocol address (IP address) is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication. An IP address serves two principal functions: host or network interface identification and location addressing.

Keylogger software

Keystroke logging, often referred to as keylogging or keyboard capturing, is the action of recording (logging) the keys struck on a keyboard, typically covertly, so that the person using the keyboard is unaware that their actions are being monitored.[7]

[7] *"Keylogger"* Oxford dictionaries

Malware

There are many current forms of malware, which has been defined by the Organization for Economic Cooperation and Development as "a general term for a piece of software inserted into an information system to cause harm to that system or other systems, or to subvert them for use other than that intended by their owners."8 Commonly-known forms include worms, viruses, and trojans. Current forms of malware can steal data by copying it and sending it to another address; they can manipulate data; they can hinder the operation of computer systems, including those that control critical infrastructures; ransomware can delete, suppress or block access to data; and specially-tailored malware can target specified computer systems[9]

Metadata

Is data providing information about one or more aspects of the data, such as:

1. Means of creation of the data
2. Purpose of the data
3. Time and date of creation
4. Creator or author of the data
5. Location on a computer network where the data was created
6. Standards used (i.e. uniform engineering or technical criteria, methods, processes and practices)

Phishing

The attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication[10]

Ransomware

A type of malicious software that blocks access to victim's data or threatens to publish or delete it until a ransom is paid.

[8] http://www.oecd.org/internet/ieconomy/40724457.pdf

[9] T-CY Guidance Notes – 1 March 2017 p 22

[10] *Ramzan, Zulfikar (2010) Phishing attacks and countermeasures - In Stamp, Mark & Stavroulakis, Peter Handbook of Information and Communication Security Springer.*

Reciprocity

Also known as mutuality, reciprocity in this context means a requested state recognizes the same investigative and court processes that the requesting state can use domestically.

Sexting

Sending, receiving, or forwarding sexually explicit messages, photographs or images

Spam

Unsolicited bulk email, where a message is sent to a significant number of email addresses, where the recipient's personal identity is irrelevant because the message is equally targeted at many other recipients without distinction[11]

Spear phishing

Phishing attempts targeted at specific individuals or corporate entities- This technique is by far the most successful on the internet today, accounting for 91% of attacks[12]

Tor

Free software for enabling anonymous communication – the name is derived from an acronym for the original software project name "*The Onion Router*"[13]

Traffic data

Information that includes records identifying with whom a subscriber communicated, what websites a subscriber visited and similar information about a user's online activity

[11] T-CY Guidance Notes – 1 March 2017 p 24

[12] Debbie Stephenson (27 July 2014) Spear Phishing: Who's Getting Caught?

[13] Tor Project: FAQ www.torproject.org

Uniform Resource Locator (URL)

A URL is one type of Uniform Resource Identifier; the generic term for all types of names and addresses that refer to objects on the World Wide Web.

Introduction

Cybercrime, or computer related crime, is a crime that involves a computer and a network.[14] A computer may have been used in the commission of a crime, or it may be the target.[15] The network will consist of more than two computer systems[16] and can be a local network or a wider area network.

Cybercrime is a global phenomenon due to increasing numbers of Information and Communication Technology (ICT) devices connected to the internet. In 2016, it was estimated that the cost of cybercrime could be as high as $2.1 trillion USD globally by 2019.[17] Upwards of 80 per cent of cybercrime acts are estimated to originate in some form of organized crime, with cybercrime black markets established, computer infection, botnet management, harvesting of personal and financial data, data sale, and 'cashing out' of financial information.[18] The 12 May 2017 Wannacry ransomware attack demonstrated the global impact of cybercrime - estimated to have affected 200,000 computers in 150 countries.

The sharp increase in cyber criminality is mainly due to the internet creating vast opportunities for organised criminals to accumulate vast profits through fraudulent schemes. A traditional law enforcement approach of arresting a suspect, getting an admission, charging and placing before the court is outdated. With cybercrime, the suspect maybe out of the jurisdiction, so consideration will have to be given at an early stage to admissibility of evidence obtained through

special investigative techniques,[19] offence/s to be charged, mutual legal assistance, extradition, and expert reports. Such investigations are timely, complex and costly. Cybercriminals take advantage when the criminal law has not adapted to the online environment and law enforcement officers are ill equipped with the necessary tools to properly investigate. The purpose of this paper is to review the context of cybercrime in the Southern Partner Countries (SPCs), and by identifying legislative gaps, make recommendations to enhance their legal frameworks, investigation procedures and international cooperation.

Cybercrime in the SPCs

A review of cybercrime in the MENA region in 2012[20] identified five fundamental challenges:

1. **Responsibility:** No one Government agency has the lead in drafting or updating cybercrime laws.
2. **Legislation:** Either non-existant or poorly drafted without consideration of the international element and requirement for specific investigative tools

[14] R. Moore (2005) Cyber crime: Investigating High-Technology Computer Crime

[15] Warren G. Kruse, Jay G. Heiser (2002) Computer forensics: incident response essentials

[16] i.e. a complete, working computer. Computer systems will include the computer along with any software and peripheral devices that are necessary to make the computer function http://www.webopedia.com/TERM/C/computer_system.html

[17] https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion

[18] ibid

[19] Article 20 of the UN Convention on Transnational Organised Crime (UNTOC) refers to special investigation techniques, including '*electronic or other forms of surveillance and undercover operations*'.

[20] Mohamed N. El-Guindy (2012) Cybercrime Challenges in the Middle East

3. **Technical capabilities:** Law enforcement officers have an inadequate understanding of securing integrity of cyber related evidence
4. **Organizational structure:** There is a lack of a specific agency dedicated to the enforcement of cybercrime and developing strategies for technological advancement.
5. **Education:** There are few public campaigns to raise awareness of the prevelance of cybercrime or training for law enforcement to ensure they are aware of current trends and threats

Some SPCs have responded to these challenges:

1. Israel has a National Cyber Event Readiness Team (CERT) – part of the National Cyber Defence Authority, has acceded to the Budapest Convention and has a specific cybercimes law (Computers Law 1995).
2. The Palestinian Public Prosecution established a specialist unit in February 2017 and the Palestinian Police has an electronic and cybercrime tracking department.
3. Egypt has the Department of Computer and Network Crimes to counter cyber threats
4. Jordan has recently updated its legislation with the Cybercrime Law No. 27 of 2015
5. Algeria has a government agency, the national body for the prevention and fight against ICT-related offenses established by Presidential Decree 15-261 of 08-10-2015 (Official Day 53 of the year 2015), The body is responsible inter alia for proposing the national strategy for the prevention and combating of ICT-related offenses and to contribute to the updating of legal standards in this field.

Cyber Threats

A cybercrime threat report for the MENA region in 2014 identified that most cyber attacks that target ICT infrastructure were DDoS or website defacement.[21] The report further highlights the vulnerability to cyber attacks due to the lack of regulation and proper legal frameworks.[22] In addition, Africa is a continent often viewed as a safe haven for cyber criminals.[23]

The challenges raise in significance with the knowledge that 55% of households surveyed in the Arab Social Media Report have 2-5 internet enabled devices (other than computers and laptops) and another 25% have 6-10 internet connected devices.[24]

The Arab States had 161 million internet users in 2016[25] and since the Arab Spring use of social media platforms has significantly increased. Facebook has 156 million users which is an increase of over 40 million from last year.[26] Egypt gained more than 14 millions Facebook users, Algeria 9.3 milion and Morocco 5.5 million.[27] The use of Twitter is significant, with Egypt producing 152 milion tweets per month and Algeria 71

[21] Mohamed N. El-Guindy (2014) Middle East Security Threat Report

[22] Ibid.

[23] Eric Tamarkin, (20 January 2015) The AU's Cybercrime Response. A Positive Start, but Substantial Challenges Ahead, Policy Brief 73

[24] Arab Social Media Report 2017 www.arabsocialmediareport.com

[25] http://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

[26] Ibid p 33

[27] Ibid p 37

million.[28] This greater use of social media enables[29] identity theft, cyberbulling, sexting and radicalisation.[30] Significantly social media has also created a conduit for terrorist fundraising, recruitment, propoganda and use of open source information[31] for attacks.

International dimensions of cybercrime

To effectively investigate and prosecute cybercrime, close cooperation is required between States. The present system of Mutual Legal Assistance (MLA) can be complex and bureaucratic, resulting in length delays to secure evidence. This does not resonate with the quick paced nature of cybercrime, where the internet has no borders. In addition, jurisdictional issues[32] have been created through cloud computing, requiring careful consideration where formal MLA requests are sent for execution.[33] Setting up procedures for quick responses to emergency incidents, preservation of evidence, as well as requests for international cooperation, are vital.[34]

[28] Ibid p 48

[29] https://www.internetmatters.org/issues/

[30] http://www.independent.co.uk/news/world/middle-east/what-makes-people-join-isis-expert-says-foreign-fighters-are-almost-never-recruited-at-mosque-a6748251.html

[31] http://www.bbc.co.uk/news/world-middle-east-18532839

[32] See: Strategic Seminar "Keys to Cyberspace" Eurojust, The Hague, 2 June 2016 Outcome Report

[33] In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation U.S. Court of Appeals (Second Circuit) 14-2985 it was decided that a warrant issue for email content in the U.S. did not apply because the data was stored internationally and the Department of Justice should approach the Irish Government through an existing mutual legal assistance treaty to access the data. An appeal of the decision is now pending in front of the US Supreme Court.

[34] Understanding Cybercrime: Phenomena, Challenge and legal Responses (ITU) page 3

Methodology

The legal, technical and institutional challenges posed by cybercrime are global and can only be addressed through a coherent strategy, taking into account the role of different stakeholders and existing initiatives,[35] within a framework of international cooperation.[36] This paper will focus upon the legislative framework and international cooperation, consistent with international norms,[37] to tackle cybercrime in the SPCs.

This paper provides a legal and a gap analysis of cybercime in the SPCs, based upon:

1. Answers to a cybercrime questionnaire sent to each SPC
2. SPC presentations at the CrimEx sessions in Masstricht on 8 May 2017
3. Research by scientific consultants based in each SPC
4. Research conducted from online resources[38]

Legal Analysis

This paper has reviewed legislation for each SPC and ratification of international[39] and regional conventions relevant to cybercrime and will focus on three areas:

1. **Offences:** For the purposes of this paper the following offences will be considered:

   a. Acts against the confidentiality, integrity and availability of computer data or system

      – Illegal access to a computer system
      – Illegal access, interception or acquisition of computer data
      – Illegal interference with a computer system or computer data
      – Production, distribution or possession of computer misuse tools
      – Breach of privacy or data protection measures

   b. Computer related acts for personal or financial gain or harm

      – Computer related fraud or forgery
      – Computer related identity offences
      – Computer related copyright or trademark offences
      – Computer related acts causing personal harm
      – Computer related solicitation or grooming of children

[35] See International Initiatives below

[36] ITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008, page 14, available at: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.

[37] UNGA Resolution: Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructure, A/RES/64/211.

[38] This includes UN Sherloc and other available online resources and texts – see Bibliography

[39] Budapest Convention on Cybercrime of the Council of Europe, African Union Convention on Cyber Security and Personal Data Protection and Arab League Convention on Combating Information Technology Offences

c. Computer content related acts

- Computer related acts involving hate speech
- Computer related production, distribution or possession of child pornography
- Computer related acts in support of terrorism offences

2. **Procedure:** Law-enforcement agencies need appropriate powers to investigate cybercrime. Such investigations can be complex and sophisticated as perpetrators use techniques to hide their identity. These challenges mean the tools required by investigators need to be different from those used to investigate more traditional acquisitive and violent crimes. The current legislative procedures to investigate cybercrime will be reviewed.
3. **International Cooperation:** Cybercrime can cover multiple jurisdictions, perpetrators and victims can be in different states and evidence located with overseas Communication Service Providers (CSPs). Processes to enable preservation of content, disclosure of traffic data and real-time interception for trans-border investigations, using mutual legal assistance, will be reviewed.

Gap Analysis

Where gaps are identified from the legal analysis this will be reviewed alongside the Budapest Convention on Cybercrime, The Arab League Convention Combating Information Technology Offences, the African Union Convention on Cyber Security and Personal Data Protection and other precedents such as the HIPCAR Model Policy Guidelines and Legislative Texts and the International Centre for Missing and Exploited Children (ICMEC) Child Pornography Model Legislation and Global Review (8th Edition 2016)

The fact that provisions exist in criminal and penal codes for substantive offences, such as fraud, does not mean that they can be applied to acts committed over the Internet as well. The analysis of current national laws has identified gaps and made recommendations to existing legislation in the **Offences** section

Recommendations to enable effective and efficient domestic investigations, prosecutions and trial, are included in the **Procedure** section.

To enhance trans-border investigations recommendations have been provided in the **international cooperation** section. These recommendations are provided to support mutual legal assistance between the SPCs and between the SPCs and the EU Member States.

These are only suggested recommendations and the SPCs will have to determine their viability based on resources and priorities. Cybercriminality is constantly evolving, and the threats increasing, as society becomes evermore reliant on the use of information technology for all facets of daily life. The challenge is for the pace of legislative reform to meet these increased risks and to equip law enforcement with the necessary tools to investigate and enable successful prosecutions.

Context

International Approaches

A number of international organizations work constantly to analyse the latest developments in cybercrime:

United Nations

In three very recent resolutions (2322 (2016), 2331 (2016), and 2341 (2017)), the Security Council called upon Member States that evidence shall be collected and preserved so that investigations and prosecutions may occur to hold accountability of those responsible for terrorist attack. Resolution 2322 (2016) specifically noted the significant increase in the requests for cooperation in gathering digital data and evidence from the Internet, and stressed the importance of considering the re-evaluation of methods and best practices, as appropriate, in particular, related to investigative techniques and electronic evidence.

To respond to this challenge, the United Nations Counter-Terrorism Executive Directorate (CTED), the United Nations Office on Drugs and Crime (UNODC) and International Association of Prosecutors (IAP) launching in February 2018 a global initiative for Strengthening the capacity of Central Authorities (CAs), Prosecutors and Investigators in Preserving and Obtaining Electronic Evidence in counter-terrorism and related organized crime cross-border investigations.

The proposed project revolves around a structured set of tailor-made and focused activities to enhance the efficiency of MLA involving electronic evidence and strengthen the capacity of relevant authorities to interact in MLA practice and communication with CSPs for this purpose. The overall purpose and goal of the project is to strengthen the capacity of CAs, prosecutors and law enforcement personnel regarding the most up-to-date procedures for requesting electronic evidence in Counter-Terrorism and Organized Crime cases. Specific Objectives are to:

1. Make best use of available resources for MLA involving electronic evidence by ensuring that: MLA requests are prioritized only where information and evidence cannot be obtained through informal means of cooperation; clear knowledge on types of tailor-made assistance is in place; structured guidance on requesting and gathering electronic evidence is available; useful information on contact points and available counterparts, as well as contacts points of CSPs, to allow for speedier communication and coordination is also available and ready for use.
2. Foster cooperation and promote communication among CAs, prosecutors and investigators from various jurisdiction, including with CSPs.

Proposed activities for a three year period would include 1) the creation of a Database of Central National Authority for Terrorist Cases; 2) the organization of two (2) Expert Group Meetings on Requesting and Gathering Electronic Evidence; 3) the compilation of country-specific focal points, legal frameworks and practical requirements for informal (police to police and prosecutor to prosecutor) and formal MLA cooperation; 4) the creation of a global specialised network and database of specialist counter-terrorism prosecutors; 5) outreach to Communication Service Providers, collection of points of contacts and internal rules for cooperation with law enforcement and creation of a database with such information; 6) the organization of seven (7) Regional Workshops respectively on Central and South Asia/South East Asia, Middle East and North Africa and Sub-Saharan Africa and Latin America and 7) the elaboration of a E-learning training curriculum for national criminal justice training institutions, dealing with Requesting and Gathering Electronic Evidence, including from CSPs. To complement this initiative - EuroMed Police, EuroMed Justice and CTED are collaborating to draft a digital evidence Guide for the SPCs (with a focus on MLA with the U.S. CSPs) for counter-terrorism investigations and prosecutions.

Council of Europe

In 1996 the European Committee on Crime Problems established a committee of experts[40] that between 1997 and 2000 drafted a Convention on Cybercrime. This became known as the Budapest Convention on Cybercrime[41] and is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception.[42] Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation. As of May 2017, 55 states have ratified the convention, while a further four states had signed the convention but not ratified it.[43] The Convention is supported by international organizations, such as Interpol.[44] Albeit, the Budapest Convention's impact has been questioned[45] with only eight states outside the Council of Europe having ratified[46] and limitations on its application to the changing cybercrime environment, for example interception of voice-over-IP (VoIP) communication, jurisdiction issues with the cloud,[47] the admissibility of digital evidence[48] and procedures to deal with the emerging use of encryption technology and means of anonymous communication. The Convention has not been amended, with the only addition being the First Additional Protocol.[49]

[40] Explanatory Report of the Convention on Cybercrime (185), No. 10

[41] The full text of Convention 185 (Convention on Cybercrime), the First Additional Protocol and the list of signatures and ratifications see: www.coe.int

[42] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

[43] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=Sv9dObc4 - please note the list is not up to date as Morocco ratified in 2012

[44] Interpol highlighted the importance of the Convention on Cybercrime in the resolution of the 6th International Conference on Cyber Crime, Cairo: "*That the Convention on Cybercrime of the Council of Europe shall be recommended as providing a minimal international legal and procedural standard for fighting cyber crime. Countries shall be encouraged to consider joining it. The Convention shall be distributed to all Interpol member countries in the four official languages*", available at: www.interpol.com/Public/TechnologyCrime/Conferences/6thIntConf/Resolution.asp

[45] For more information on the achievements and shortcomings see: Gercke, 10 Years Convention on Cybercrime, Computer Law Review International, 2011, page 142 et seq.

[46] Morocco (2012), Australia (2013), Canada (2015), Chile (2017), Israel (2016), Japan (2012), Sri Lanka (2015) and the United States (2007)

[47] See: Strategic Seminar "Keys to Cyberspace" Eurojust, The Hague, 2 June 2016 Outcome Report

[48] Lange/Nimsger (2004) Electronic Evidence and Discovery and Whitcomb, An Historical Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, No. 1.

[49] Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, ETS No. 189, available at: https://www.coe.int/en/web/conventions/full-list/-/conventions/webContent/en_GB/7836079 29 States are parties and 13 States have signed, San Marino being the latest on 19 May 2017 https://www.coe.int/en/web/cybercrime/-/signature-san-marino-of-the-protocol-on-xenophobia-and-racism-

One of the fundamental aspects of the Budapest Convention is the provision of a 24/7 Network[50] to enable effective investigation and preservation of evidence.[51] Two studies in 2008[52] and 2009[53] showed that states that had ratified the Convention were still to establish contact points, despite this being a mandatory requirement. It can be a challenge for some states to have a single point of contact (SPOC) available at all times when investment in cybercrime investigations is minimal. Although, due to the speed of cybercriminality a SPOC is an essential element of an effective international framework.

African Union

It was decided during the extra-ordinary conference of the African Union Ministers in charge of Communication and Information Technologies, in Johannesburg in 2009, that the African Union Commission should – jointly with the UN Economic Commission for Africa – develop a legal framework for African countries that addresses electronic transactions, cyber security and data protection.[54]

The African Union (AU) presented the Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa in 2011.[55] In July 2014 the AU adopted the Convention on Cybersecurity and Personal Data Protection (AUC). By mid-2016, only 12 of the 54 African countries had basic substantive or procedural law provisions on cybercrime and electronic evidence in place. Many others were in the process of drafting legislation with the African Union and Budapest Conventions serving as guidance.

A comparative analysis of the AUC shows that it criminalizes some, but not all of the conduct foreseen under the Budapest Convention. Most offences under the AUC are missing appropriate mens rea elements, and could criminalize legitimate conduct of law enforcement authorities and other conduct that should be lawful under international best practice.[56] Moreover, the AUC does not provide for the full set of procedural powers for investigating and prosecuting cybercrime and securing electronic evidence in domestic investigations – for example production orders, which are crucial to obtain data from CSPs are not included.[57] Further, the AUC does not constitute a legal basis for international cooperation on cybercrime and electronic evidence.[58]

Arab League and Gulf Cooperation Council

The Arab Treaty on Countering Information Technology Offences ('CITO') was adopted in December 2010 and entered into force in February 2014. To date Algeria, Jordan, UAE, Sudan, Iraq, PA, Qatar, Kuwait and Egypt have ratified CITO. The main obligation of CITO is to implement domestic legislation to criminalise and procedural powers to investigate cybercrime offences.

[50] Article 35

[51] See Explanatory Report to the Convention on Cybercrime, No. 298.

[52] Verdelho (2008) The effectiveness of international cooperation against cybercrime

[53] The Functioning of 24/7 points of contact for cybercrime, 2009

[54] For more information see: African Union, Oliver Tambo Declaration, Johannesburg 2009, available at: www.uneca.org/aisi/docs/AU/The%20Oliver%20Tambo%20Declaration.pdf

[55] The Draft Convention is available for download at: www.itu.int/ITUD/projects/ITU_EC_ACP/hipssa/events/2011/WDOcs/CA_5/Draft%20Convention%20on%20Cyberlegislation%20in%20Africa%20Draft0.pdf

[56] Comparative Analysis of the Malabo Convention of the African Union and the Budapest Convention on Cybercrime 20 November 2016

[57] Ibid

[58] Ibid

As outlined above re the AUC - CITO lacks mens rea for certain offences. For example Articles 6, 8,[59] 9[60] do not refer to "*without right*".[61] Further, Article 6 criminalizes "*illegal access*" but does not provide a definition of what illegal access is. Significantly CITO does not include an offence of system interference,[62] which aims at criminalising the intentional hindering of the lawful use of computer systems including telecommunications facilities by using or influencing computer data.

In relation to international cooperation Article 34[63] does provide for CITO to be the basis for mutual legal assistance and Article 31[64] for extradition if there is no applicable bilateral treaty. Dual criminality is an essential prerequisite to the provision of any mutual legal assistance under Article 32(5). This is against international norms where dual criminality has a broader definition for MLA[65] and where it isn't required under the Budapest Convention[66] for less intrusive powers to ensure that cybercriminality evidence is preserved.

Other significant international provisions include the disclosure of information under Article 33[67] by law enforcement to another party to CITO that can be used proactively by a receiving state and maintaining confidentiality of any MLA request.[68] There is also provision under Article 43 for a, "…*specialized body dedicated 24 hours a day to ensure the provision of prompt assistance for the purposes of investigation, procedures related to information technology offences or gather evidence in electronic form regarding a specific offence.*"[69]

CITO does not include provision for the real-time collection of traffic data or content through MLA.[70] This could impede international investigations where IP address collection or real-time content may disclose the location of offenders to prevent cybercrimes. This gap can be easily bridged through the adoption of Article 34 of the Budapest Convention.

HIPCAR

The Enhacing Competitiveness in the Caribbean through the Harmonization of ICT Policies Legislation and Regulatory Procedures has provided model cybercrime legislation for 15 Caribbean countries in the Group of African, Caribbean and Pacific States (ACP).[71] The project has been managed by the International Telecommunications Union (ITU) and a global steering committee with representatives from the European Commission. The model legislative texts were drafted following a legal analysis of national legislation, international best practice from the UN, OECD, EU and legislation from the UK, Australia, Malta and Brazil as benchmarks. Whilst the model legislative text has been drafted taking into account the specific needs of small island states, it is a useful guideline for those states with limited or no cybercrime legislation.

[59] Offence against the Integrity of Data – akin to Article 4 of the Budapest Convention re Data Interference

[60] Offence of Misuse of Information Technology Means – akin to Article 6 of the Budapest Convention re Misuse of Devices

[61] Article 2 of the Budapest Convention refers to access "*without right" or unauthorized access – this means the offence would be one of strict liability and could mean that any person – law enforcement or otherwise who accesses data without consent is committing an offence.*

[62] See Article 5 of the Budapest Convention

[63] Consistent with Article 23 of the Budapest Convention

[64] Consistent with Article 24 of the Budapest Convention

[65] See Article 18(9) UNTOC

[66] For example, Article 29.3. for the preservation of stored computer data

[67] Consistent with Article 26 of the Budapest Convention

[68] Article 34(7) and Article 36 of CITO – consistent with Article 28 of the Budapest Convention

[69] It is unclear for those SPCs who have ratified CITO (Jordan, Palestine and Egypt) if they have established this *specialized body*

[70] Articles 33 and 34 of the Budapest Convention

[71] https://www.itu.int/en/ITU-D/Cybersecurity/Documents/HIPCAR%20Model%20Law%20Cybercrimes.pdf

ICMEC

The ICMEC Model Legislation and Global Review 8th Edition[72] of 2016 considers a core set of criteria to provide a legal analysis to confirm if:

1. If national legislation exists with specific regard to child pornography;
2. National legislation provides a definition of child pornography;
3. National legislation criminalizes computer-facilitated offenses;
4. National Legislation criminalizes the knowing possession of child pornography, regardless of the intent to distribute; and
5. National legislation requires CSPs to report suspected child pornography to law enforcement or to some other mandated agency.

[72] https://www.icmec.org/wp-content/uploads/2016/02/Child-Pornography-Model-Law-8th-Ed-Final-linked.pdf

Legal and Gap Analyses

A legal analysis is provided in this section of current national laws and a gap analysis with recommendations for each SPC.[73]

Algeria

Algeria has ratified the Arab League Convention Combating Information Technology Offences (CITO).

Offences		
International Best Practice	**National Legislation**	**Comments**
Article 2 BC – Illegal Access[74] Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system. **Section 4 HIPCAR – Illegal Access** 1. A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, accesses the whole or any part of a computer system commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.	**Penal Code – 05-09-2009**[75] **Article 394 bis** Anyone who fraudulently accesses or maintains himself in all or part of a system automated data processing, or attempts to do so.	**Legal Analysis** The national provision includes reference to "*fraudulently*" this would suggest that the perpetrator has accessed the data dishonestly – whereas the BC refers to "*without right*" on the basis access is unauthorized. The BC refers to a "*dishonest intent*" but this is the mens rea to secure data rather than the act of gaining illegal access. At present this national offence can only be committed where the perpetrator dishonestly represents the purpose for accessing. It is unclear without a definition of "*fraudulently*" if this requires an overt action or if every illegal access is deemed to be fraudulent. It is for this reason that a definition of "*fraudulent*" is required. The term "computer system" is defined in Article 2 of law 09-04 of 05-08-2009 laying down special rules relating to the prevention and the fight against the infractions linked to ICT. The offence also refers to a "*system automated data processing*" without a definition. It is unclear if this also relates to a "*computer system*" CITO refers to "*illicit access to, presence in or contact with*" without defining what these acts mean – therefore, BC and HIPCAR are to be preferred.

[73] For an overview of cybercrime-related legislation in member states and its compliance with the best practices defined by the Convention on Cybercrime, see the country profiles provided on the Council of Europe website, available at: www.coe.int/cybercrime/

[74] Article 6 CITO and Article 29(1) AUC

[75] https://www.unodc.org/res/cld/document/code-penal-2009_html/Penal_Code_Algeria_2009.pdf

Offences		
International Best Practice	**National Legislation**	**Comments**
2. A country may decide not to criminalize the mere unauthorized access provided that other effective remedies are available. Furthermore, a country may require that the offence be committed by infringing security measures or with the intent of obtaining computer data or other dishonest intent. **Section 5 HIPCAR – Illegal Remaining** 1. 1A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, remains logged in a computer system or part of a computer system or continues to use a computer system commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. 2. A country may decide not to criminalize the mere unauthorized remaining provided that other effective remedies are available. Alternatively, a country may require that the offence be committed by infringing security measures or with the intent of obtaining computer data or other dishonest intent.		**Gap Analysis** **Recommendation:** The national legislation could include programs within the definition of data as some data includes programs and other data does not. Further, to be consistent with international standards refer to access "without right" rather than fraudulently

Offences		
International Best Practice	**National Legislation**	**Comments**
Article 3 BC[76] **Illegal Interception** Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system. **Section 6 HIPCAR – Illegal Interception** 1. A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, intercepts by technical means: any non-public transmission to, from or within a computer system; or electromagnetic emissions from a computer system commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. 2. A country may require that the offence be committed with a dishonest intent, or in relation to a computer system that is connected to another computer system, or by circumventing protection measures implemented to prevent access to the content of non-public transmission.	The law No. 18-04 of 10 May 2018 laying down general rules for postal and electronic communications criminalized the violation of secrecy of correspondence transmitted by electronic means. Article 164 of this Act states as follows: "anyone who violates the secrecy of correspondence transmitted by post or by electronic means of communication, or discloses their content, publishes it, or uses it without the permission of the sender or the recipient, or reveals their existence is punishable by imprisonment from one to five years and a fine of 500,000 to 1,000,000 DA."	**Legal Analysis** This offence is essential to prosecute non-public transmissions of computer data to, from, or within a computer system that may be illegally intercepted to obtain information about a person's location (e.g. to target that person).[77] **Gap Analysis** **Recommendation:** Use the BC language in Article 3, HIPCAR section 6 as a guide - the language in Article 7 CITO is appropriate – albeit there is no definition of "*information technology data*"

[76] Article 29(2) AUC

[77] http://www.coe.int/en/web/cybercrime/guidance-notes

Offences		
International Best Practice	National Legislation	Comments
Article 7 CITO **Illicit Interception** The deliberate unlawful interception of the movement of data by any technical means, and the disruption of transmission or reception of information technology data.		
Article 4 BC[78] **Data Interference** Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm. **Section 7 HIPCAR – Illegal Data Interference** A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, does any of the following acts: • damages or deteriorates computer data; or • deletes computer data ; or • alters computer data; or • renders computer data meaningless, useless or ineffective; or • obstructs, interrupts or interferes with the lawful use of computer data; or • obstructs, interrupts or interferes with any person in the lawful use of computer data; or	**Penal Code – 05-09-2009**[79] **Article 394c** Anyone who wilfully and fraudulently: 1. designs, retrieves, assembles, makes available, disseminates or markets data that are stored, processed or transmitted by a computer system and through which the offenses set forth in this section may be committed, 2. holds, discloses, discloses, or makes any use of data obtained by any of the offenses set forth in this section.	**Legal Analysis** The use of,“*fraudulently*” is inconsistent (in fact in conflict with) the standard of the BC 4.1 “…*when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right*” (or section 7 HIPCAR) which does not require fraud to be proved.This means that conduct which constitutes an offence of data interference under the BC’s 4.1 (or section 7 HIPCAR) would not be criminalized under Art. 394c Article 394c does not include the element of suppression of computer data **Gap Analysis** **Recommendation:** Use Article 4 BC or section 7 HIPCAR as a guide for national legislation

[78] Article 29(1)(e-f) AUC

[79] https://www.unodc.org/res/cld/document/code-penal-2009_html/Penal_Code_Algeria_2009.pdf

Offences		
International Best Practice	**National Legislation**	**Comments**
- denies access to computer data to any person authorized to access it; commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. **Article 8 CITO** **Offence Against the Integrity of Data** 1. Deliberate unlawful destruction, obliteration, obstruction, modification or concealment of information technology data. 2. The Party may require that, in order to criminalize acts mentioned in paragraph 1, they must cause severe damage.		
Article 5 BC[80] **System Interference** Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data. **Section 9 HIPCAR – Illegal System Interference** 1. A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification: - hinders or interferes with the functioning of a computer system; or - hinders or interferes with a person who is lawfully using or operating a computer system;	**No equivalent**	**Legal Analysis** This offence would prevent malware that interferes with the functioning of a computer – for example computer worms - a subgroup of malware (like computer viruses). They are self-replicating computer programs that harm the network by initiating multiple data-transfer processes. They can influence computer systems by hindering the smooth running of the computer system, using system resources to replicate themselves over the Internet or generating network traffic that can close down availability of certain services (such as websites).

[80] Article 29(1)(d) AUC no equivalent in CITO

Offences		
International Best Practice	**National Legislation**	**Comments**
commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. 2. A person who intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification hinders or interferes with a computer system that is exclusively for the use of critical infrastructure operations, or in the case in which such is not exclusively for the use of critical infrastructure operations, but it is used in critical infrastructure operations and such conduct affects that use or impacts the operations of critical infrastructure the punishment shall be imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.		**Gap Analysis** **Recommendation:** Use the BC language in Article 5 or section 9 HIPCAR as a guide for national legislation. Also consider whether the prevention and prosecution of attacks against critical infrastructure needs a separate or aggravated offence (Section 9(2) HIPCAR) for example the functioning of a computer system may be hindered for terrorist purposes (e.g. hindering the system that stores stock exchange records can make them inaccurate, or hindering the functioning of critical infrastructure).[81]
Article 6 BC[82] **Misuse of Devices** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a. the production, sale, procurement for use, import, distribution or otherwise making available of: i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;	**No equivalent**	**Legal Analysis** As above for Illicit Access there is no reference to "without right" This offence will enable prosecution for the production, sale, procurement for use, import, distribution of access codes and other computerized data used to commit cybercrimes. - for example, computer systems may be accessed to facilitate a terrorist attack by interfering with a country's electrical power grid. Any offence would also have to consider those devices that have a legitimate as well as being put to criminal use ("dual use") – this should include the BC language of "primarily adapted" **Gap Analysis** **Recommendation:** Use the BC language in Article 6 or section 10 HIPCAR as a guide for national legislation.

[81] http://www.coe.int/en/web/cybercrime/guidance-notes

[82] Article 9 CITO and Article 29(1)(h) AUC

Offences		
International Best Practice	**National Legislation**	**Comments**
ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b. the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3. Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article		Please note that HIPCAR provides the option of listing the devices in a schedule if deemed appropriate – this could be restrictive and require updating with technological progress. The national law should provide a reasonable excuse so law enforcement can use devices for special investigation techniques – see the language at Article 6.2. BC or section 10(2) HIPCAR as a guide.

Offences		
International Best Practice	**National Legislation**	**Comments**
Section 10 HIPCAR – Illegal Devices 1. A person commits an offence if the person: a. intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, produces, sells, procures for use, imports, exports, distributes or otherwise makes available: i. a device, including a computer program, that is designed or adapted for the purpose of committing an offence defined by other provisions of Part II of this law; or ii. a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed; with the intent that it be used by any person for the purpose of committing an offence defined by other provisions of Part II of this law; or b. has an item mentioned in subparagraph (i) or (ii) in his or her possession with the intent that it be used by any person for the purpose of committing an offence defined by other provisions of part II of this law commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.		

Offences		
International Best Practice	**National Legislation**	**Comments**
2. This provision shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 is not for the purpose of committing an offence established in accordance with other provisions of Part II of this law, such as for the authorized testing or protection of a computer system. 3. A country may decide not to criminalize illegal devices or limit the criminalization to devices listed in a Schedule.		
Article 7 BC **Computer Related Forgery** Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.	**No equivalent**	**Legal Analysis** Incorporation of BC article 7, section 11 HIPCAR or section 29(2)(b) AUC is advised to protect against this offending which could include phishing and spear phishing For example, computer data (such as the data used in electronic passports) may be input, altered, deleted, or suppressed with the result that inauthentic data is considered or acted upon for legal purposes as if it were authentic.[83] Section 11(2) HIPCAR also provides for the sending of multiple electronic email messages as an aggravated offence. The language in Article 10 CITO has no reference to any dishonest intent and requires harm to be caused – the language in BC and HIPCAR is to be preferred as it does not require harm to be caused. BC and HIPCAR only requires that the "*inauthentic data*" data is "*considered*" **Gap Analysis** **Recommendation:** Use the BC language in Article 7, section 11 HIPCAR or 29(2)(b) AUC as a guide for national legislation

[83] http://www.coe.int/en/web/cybercrime/guidance-notes

Offences		
International Best Practice	**National Legislation**	**Comments**
Section 11 HIPCAR – Computer-related Forgery 1. A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification inputs, alters, deletes, or suppresses computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. 2. If the abovementioned offence is committed by sending out multiple electronic mail messages from or through computer systems, the penalty shall be imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. **Article 10 CITO** **Offence of Forgery** The use of information technology means to alter the truth of data in a manner that causes harm, with the intent of using them as true data. **Article 29(2)(b) AUC** Intentionally input, alter, delete, or suppress computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable and intelligible. A Party may require intent to defraud, of similar dishonest intent, before criminal liability attaches		

Offences		
International Best Practice	**National Legislation**	**Comments**
Article 8 BC[84] **Computer Related Fraud** Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a. any input, alteration, deletion or suppression of computer data, b. any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person. **Section 12 HIPCAR – Computer-related Fraud** A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification causes a loss of property to another person by: • any input, alteration, deletion or suppression of computer data; • any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person the penalty shall be imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.	**Penal Code – 05-09-2009** **Article 394 ter** Anyone who fraudulently enters data into an automated processing system or fraudulently deletes or modifies the data it contains	**Legal Analysis** Whilst "*fraudulently*' in in Article 394 of the national legislation does provide a certain degree of protection, the absence of committing this conduct without authorization is missing and may create uncertainty. The term "*computer data*" is defined in Article 2 of law 09-04 of 05-08-2009 laying down special rules relating to the prevention and the fight against infractions linked to ICT There is no definition of "*automated processing system*" and this may create uncertainty. The language in Article 11 CITO and 29(2)(d) AUC is vague with no reference to any dishonest intent and requires some form of "*harm*" (CITO) or "benefit" (AUC) without defining what this is **Gap Analysis** **Recommendation:** Providing definition for "*automated processing system*" and including "*without authorization*" – the language in BC or HIPCAR for this offence is a good guide for national legislation

[84] Article 11 CITO and Article 29(2)(d) AUC

Offences		
International Best Practice	**National Legislation**	**Comments**
Article 9 BC[85] **Content Related Offences (e.g. child pornography)** **Section 13 HIPCAR – Child Pornography**	**Penal Code – 05-09-2009** **Article 333 bis 1** Imposes a criminal penalty for anyone who represents, by any means, a person under eighteen (18) years participating in explicit sexual activities, real or simulated, or represents the sexual organs of a minor, for primarily sexual purposes, or is involved in the production, distribution, dissemination, propagation, import, export, offer, sale or possession of pornographic material featuring minors.	**Legal Analysis** This is an essential offence in order to protect children from harm by criminalizing the distribution, transmitting, making available, offering, producing and possession of indecent images of children. **Gap Analysis** **Recommendation:** The ICMEC Global review confirms the national legislation satisfies its core criteria[86]
Article 10 BC[87] **Infringement of Copyright** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.	**Ordinance 03-05 of 19-07-2003 on copyright and neighboring rights and Ordinance 03-07 of 19- 07-2003 relating to patents.**	**Legal Analysis** Law enforcement internationally utilizes digital copyright offences as additional criminal conduct to investigate and prosecute several forms of cybercrime (which include crimes such as phishing, electronic fraud, electronic forgery, fraudulent websites and data theft/data breaches). One of the underlying offences in many of these cases tends to be infringement of digital copyright. The Sony cyber attack88 is only one recent example where offences and powers related to cybercrime, data theft/corporate espionage and copyright infringement came together to complement one another. The absence of any provisions relating to intellectual property would constitute a failure to protect the innovation in the 21st century of the SPCs, businesses and citizens. There is legal protection for digital works, databases and computer programs in Ordinance 03-05 of 19-07-2003 on copyright and neighboring rights and Ordinance 03-07 of 19- 07-2003 relating to patents.

[85] Article 12 CITO and Article 29(3)(a-d) AUC

[86] ICMEC Global Review page 18

[87] no equivalent in AUC and HIPCAR

[88] https://en.wikipedia.org/wiki/Sony_Pictures_hack

Offences		
International Best Practice	**National Legislation**	**Comments**
2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 3. A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article. **Article 17 CITO - Offenses Related to Copyright and Adjacent Rights** Violation of copyright as defined according to the law of the State Party, if the act is committed deliberately and for no personal use, and violation of rights adjacent to the relevant copyright as defined according to the law of the State Party, if the act is committed deliberately and for no personal use.		

Offences		
International Best Practice	**National Legislation**	**Comments**
Article 11 BC[89] **Aiding and Abetting** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed. 2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention. **Article 19 CITO - Attempt at and Participation in the Commission of Offences** 1. Participation in the commission of any of the offences set forth in this chapter with the intention to commit the offence in the law of the State Party. 2. Attempt at the commission the offences set forth in Chapter II of this convention. 3. A State Party may reserve the right to not implement the second paragraph of this Article totally or partly.	**Criminal Code** Article 394	**Legal Analysis** Aiding and abetting others to commit offences is essential in order to prosecute those who may have provided assistance or encouraged cybercrimes to take place. Article 394 of the Criminal Code punishes the participation and complicity in the commission of offenses against computerized data processing systems.

[89] Article 29(2)(f) AUC

Offences		
International Best Practice	**National Legislation**	**Comments**
Article 12 BC[90] **Corporate liability** 1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on: a. a power of representation of the legal person; b. an authority to take decisions on behalf of the legal person; c. an authority to exercise control within the legal person. 2. In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority. 3. Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative. 4. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.	**Criminal Code** Article 394	**Legal Analysis** This provision is an essential element so that legal persons (e.g. corporate entities) acting on behalf of natural persons have criminal liability. The liability of the legal person in the commission of offenses against computerized data processing systems is laid down in Article 394 of the Criminal Code.

[90] Article 20 CITO and Article 30(2) AUC

Offences

International Best Practice	National Legislation	Comments
Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems **Article 3[91] – Dissemination of racist and xenophobic material through computer systems** Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: 1. Distributing, or otherwise making available, racist and xenophobic material to the public through a computer system. 2. A Party may reserve the right not to attach criminal liability to conduct as defined by paragraph 1 of this article, where the material, as defined in Article 2, paragraph 1, advocates, promotes or incites discrimination that is not associated with hatred or violence, provided that other effective remedies are available. 3. Notwithstanding paragraph 2 of this article, a Party may reserve the right not to apply paragraph 1 to those cases of discrimination for which, due to established principles in its national legal system concerning freedom of expression, it cannot provide for effective remedies as referred to in the said paragraph 2.	**No equivalent**	**Legal Analysis** The AUC Article 3(1)(e) which includes the creation of and downloading racist and xenophobic material through a computer system rather than merely disseminating or making such material available, does not include an intent or "*without right*" – the BC language is to be preferred. **Gap Analysis** **Recommendation:** Use the BC language in Article 3 Additional Protocol as a guide for national legislation

[91] Article 29(3)(e) AUC no equivalent in CITO

PORTADA INDEX

Offences		
International Best Practice	**National Legislation**	**Comments**
Additional Protocol **Article 4[92] – Racist and xenophobic motivated threat** Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: threatening, through a computer system, with the commission of a serious criminal offence as defined under its domestic law, (i) persons for the reason that they belong to a group, distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors, or (ii) a group of persons which is distinguished by any of these characteristics.	**No equivalent**	**Gap Analysis** **Recommendation:** Use the BC language in Article 4 Additional Protocol as a guide for national legislation
Additional Protocol **Article 5[93] - Racist and xenophobic motivated insult** Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: 1. insulting publicly, through a computer system, (i) persons for the reason that they belong to a group distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors; or (ii) a group of persons which is distinguished by any of these characteristics.	**No equivalent**	**Gap Analysis** **Recommendation:** Use the BC language in Article 5 Additional Protocol as a guide for national legislation

[92] Article 29(3)(f) AUC no equivalent in CITO

[93] Article 29(3)(g) AUC no equivalent in CITO

Offences		
International Best Practice	**National Legislation**	**Comments**
2. A Party may either: arequire that the offence referred to in paragraph 1 of this article has the effect that the person or group of persons referred to in paragraph 1 is exposed to hatred, contempt or ridicule; or breserve the right not to apply, in whole or in part, paragraph 1 of this article.		
Additional Protocol **Article 6[94] - Denial, gross minimisation, approval or justification of genocide or crimes against humanity** Each Party shall adopt such legislative measures as may be necessary to establish the following conduct as criminal offences under its domestic law, when committed intentionally and without right: 1. distributing or otherwise making available, through a computer system to the public, material which denies, grossly minimises, approves or justifies acts constituting genocide or crimes against humanity, as defined by international law and recognised as such by final and binding decisions of the International Military Tribunal, established by the London Agreement of 8 August 1945, or of any other international court established by relevant international instruments and whose jurisdiction is recognised by that Party.	**No equivalent**	**Gap Analysis** **Recommendation:** Use the BC language in Article 6 Additional Protocol as a guide for national legislation

[94] Article 29(3)(h) AUC no equivalent in CITO

Offences		
International Best Practice	**National Legislation**	**Comments**
2. A Party may either a. require that the denial or the gross minimisation referred to in paragraph 1 of this article is committed with the intent to incite hatred, discrimination or violence against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors, or otherwise b. reserve the right not to apply, in whole or in part, paragraph 1 of this article.		
Additional Offences to Review		
Identity-related Crimes **Section 14 HIPCAR** A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification by using a computer system in any stage of the offence, intentionally transfers, possesses, or uses, without lawful excuse or justification, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a crime, commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.		**Legal Analysis** This offence covers the preparation phase of an identity –related crime of dishonesty **Gap Analysis** **Recommendation:** Inclusion in domestic legislation is advisable.

Offences		
International Best Practice	**National Legislation**	**Comments**
Disclosure of Details of an Investigation **Section 16 HIPCAR** An Internet service provider who receives an order related to a criminal investigation that explicitly stipulates that confidentiality is to be maintained or such obligation is stated by law and intentionally without lawful excuse or justification or in excess of a lawful excuse or justification discloses: • the fact that an order has been made; or • anything done under the order; or • any data collected or recorded under the order; commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.	**Law No. 09-04 of 14 Chaâbane 1430 corresponding to 5 August 2009 laying down specific rules on the prevention and the fight against infringements related to information and communication technologies** **Article 10**	**Legal Analysis** Article 10 of Law 09-04 establishes the possibility to prosecute the communication service providers (as legal persons) or natural persons undermining the confidentiality of the operations if the judicial or law enforcement authorities so request, for breach of the secrecy of investigation.
Failing to Permit Assistance **Section 17 HIPCAR** 1. A person other than the suspect who intentionally fails without lawful excuse or justification or in excess of a lawful excuse or justification to permit or assist a person based on an order as specified by sections 20 to 2295 commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. 2. A country may decide not to criminalize the failure to permit assistance provided that other effective remedies are available.		**Legal Analysis** This offence relates to persons, with specific knowledge of relevant evidence, who refuse to assist. Often law enforcement will be reliant upon such persons to secure evidence in cyber investigations. A separate offence is the failure to provide passwords or access to codes to encrypted devices or data (i.e. "key to protected information") – section 53 of the UK Regulation of Investigatory Powers Act 2000 (RIPA) [96] provides for a criminal offence for persons who fail to comply with a section 49 RIPA Notice to disclose the "key" **Gap Analysis** **Recommendation:** Inclusion in domestic legislation is advisable.

[95] Search and seizure, assistance and production orders

[96] http://www.legislation.gov.uk/ukpga/2000/23/section/53

Offences		
International Best Practice	**National Legislation**	**Comments**
Cyber Stalking **Section 18 HIPCAR** A person, who without lawful excuse or justification or in excess of a lawful excuse or justification initiates any electronic communication, with the intent to coerce, intimidate, harass, or cause substantial emotional distress to a person, using a computer system to support severe, repeated, and hostile behavior, commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.		**Legal Analysis** This offence criminalizes those who harass persons online– some jurisdictions may have non-computer related harassment offences – but this offence is recommended for those crimes committed online. **Gap Analysis** **Recommendation:** Inclusion in domestic legislation is advisable.
Grooming Children Online **Dutch Criminal Code 248e** The person who proposes to arrange a meeting, by means of an automated work or by making use of a communication service, to a person of whom he knows, or should reasonably assume, that such person has not yet reached the age of sixteen, with the intention of committing indecent acts with this person or of creating an image of a sexual act in which this person is involved, will be punished with a term of imprisonment of at most two years or a fine of the fourth category, if he undertakes any action intended to realise that meeting. **Canadian Criminal Code** **Section 172.1** 1. Every person commits an offence who, by a means of telecommunication, communicates with		**Legal Analysis** To prove the Dutch offence a meeting for sexual purposes is required with supporting evidence of online chat history with sexual intent; request for a meeting with evidence this was planned (i.e. date and place). The purpose of the Canadian law is to prevent grooming by predatory adults of children online. This offence does not require the sexual offence to have occurred. This means the accused does not need to have actually gone to meet the victim in person. The offence is committed before any actions are taken to commit the substantive offence. **Gap Analysis** **Recommendation:** Inclusion in domestic legislation is advisable to criminalise this preparatory behaviour before a sexual offence is committed

Offences		
International Best Practice	National Legislation	Comments
a. a person who is, or who the accused believes is, under the age of 18 years, for the purpose of facilitating the commission of an offence under subsection 153(1), section 155, 163.1, 170 or 171 or subsection 212(1), (2), (2.1) or (4) with respect to that person; b. a person who is, or who the accused believes is, under the age of 16 years, for the purpose of facilitating the commission of an offence under section 151 or 152, subsection 160(3) or 173(2) or section 271, 272, 273 or 280 with respect to that person; or c. a person who is, or who the accused believes is, under the age of 14 years, for the purpose of facilitating the commission of an offence under section 281 with respect to that person. Punishment 2. Every person who commits an offence under subsection (1) is guilty of a. is guilty of an indictable offence and is liable to imprisonment for a term of not more than 10 years and to a minimum punishment of imprisonment for a term of one year; or b. is guilty of an offence punishable on summary conviction and is liable to imprisonment for a term of not more than 18 months and to a minimum punishment of imprisonment for a term of 90 days.		

Offences		
International Best Practice	**National Legislation**	**Comments**
Presumption re age 3. Evidence that the person referred to in paragraph (1) (a), (b) or (c) was represented to the accused as being under the age of eighteen years, sixteen years or fourteen years, as the case may be, is, in the absence of evidence to the contrary, proof that the accused believed that the person was under that age. No defence 4. It is not a defence to a charge under paragraph (1) (a), (b) or (c) that the accused believed that the person referred to in that paragraph was at least eighteen years of age, sixteen years or fourteen years of age, as the case may be, unless the accused took reasonable steps to ascertain the age of the person.		

Procedure		
International Best Practice	**National Legislation**	**Comments**
Article 19 BC[97] **Search and seizure of stored computer data** 1. 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a. a computer system or part of it and computer data stored therein; and b. a computer-data storage medium in which computer data may be stored in its territory. 2. Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a. seize or similarly secure a computer system or part of it or a computer-data storage medium;	**Law No. 09-04 of 14 Chaâbane 1430 corresponding to 5 August 2009 laying down specific rules on the prevention and the fight against infringements related to information and communication technologies[98]** **Article 3** In accordance with the rules laid down in the Code of Criminal Procedure and this Law and subject to the legal provisions guaranteeing the secrecy of Correspondence and communications, provision may be made for technical requirements for the protection of public order or for the purposes of investigations or judicial information in progress to carry out electronic communications surveillance operations, Collection and recording of their content in real time, as well as **searches and seizures in a computer system.** **Article 4** The monitoring operations provided for Article 3 may be carried out in the event of the following: A. to prevent offenses classified as terrorist or subversive acts and offenses against the security of the State.	**Legal Analysis** The Article 3 power is to search and seize rather than to gain access. In the BC Explanatory Report, *“Search”* means to seek, read, inspect or review data. It includes the notion of searching for data and searching of (examining) data. The word “access” has a neutral meaning and reflects more accurately computer terminology.[99] Article 5 does refer to “*access*” but this should be consistently referred to in Article 3 – Article 26 CITO does refer to “*access*” Articles 3 and 5 also refer to a “*computer system*” and Article 5 to ‘*computer data stored*” and a “*computer storage system*” – therefore - only **stored** data can be seized. Article 2 of Law 09-04 defines “*computer system*”, “*computer data*”, “*service providers*”, “*traffic data*”, and “*electronic communications*” in accordance with the language of the BC and CITO. **Gap Analysis** **Recommendations:** The national legislation should consistently refer to *access* Article 4 restricts the search and seizure provisions to certain categories of offence – this means that many cybercrimes that are not crimes against national security or terrorist related will not have relevant procedural powers to search and seize (only in the context of prevention) Article 5 goes beyond Article 19 BC and section 20 HIPCAR in that powers to search connected systems can be extended to any computer in the world based upon reciprocity – this provision will also be restricted on the basis that it will only apply to the category of offences in Article 4

[97] Article 3 AUC

[98] https://www.unodc.org/res/cld/document/dza/2009/loi_n_09-04_du_14_chaabane_1430_correspondant_au_5_aout_2009_portant_regles_particulieres_relatives_a_la_prevention_et_a_la_lutte_contre_les_infractions_liees_aux_technologies_de_linformation_et_de_la_communication_html/Loi_prevention_et_lutte_contre_les_infractions_liees_aux_technologies_de_linformation_et_de_la_communication.pdf

[99] Explanatory Report BC paragraph 191

Procedure		
International Best Practice	**National Legislation**	**Comments**
b. make and retain a copy of those computer data; c. c maintain the integrity of the relevant stored computer data; d. render inaccessible or remove those computer data in the accessed computer system. 4. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and2. 5. The powers and procedures referred to in this article shall be subject to Articles 14 and 15. **Section 20 HIPCAR – Search and Seizure** 1. If a [judge] [magistrate] is satisfied on the basis of [information on oath] [affidavit] that there are reasonable grounds [to suspect] [to believe] that there may be in a place a thing or computer data: • that may be material as evidence in proving an offence; or • that has been acquired by a person as a result of an offence; the [judge] [magistrate] [may] [shall] issue a warrant authorizing a [law enforcement] [police] officer, with such assistance as may be necessary, to enter the place to search and seize the thing or computer data including search or similarly access:	B. where there is information on a likely impairment of a computer system representing a threat to public order, national defense, State institutions or the national economy; C. for the purposes of investigations and judicial information where it is difficult to achieve results relevant to ongoing research without the use of electronic surveillance; D. in the execution of requests for international judicial assistance the surveillance operations mentioned above may only be carried out with the written authorization of the competent judicial authority. In the case referred to in paragraph (a) of this Article, the authorization shall be issued to the judicial police officers under the authority referred to in Article 13 below by the Attorney General of the Court Of Algiers, for a renewable period of six (6) months, on the basis of a report indicating the nature of the technical process used and the objectives to which it refers. Under the penalties provided for in the Criminal Code with regard to the invasion of the privacy of others, technical devices set up for the purposes described in paragraph A. of this Article shall be directed exclusively to the collection and recording of data relating to the prevention and control of terrorist acts and attacks on State security.	The power to access and search should be wider than the present restricted categorization of offences to include cybercrime offences in Law 09-04. Article 6 refers to ensuring the copying, original data content and integrity of any evidence seized. Although it does not refer to rendering the data inaccessible to prevent any further offending. BC Article 19.3.d. language is considered for inclusion to ensure the seized data is rendered inaccessible to prevent any other use. Article 5 refers to the "*requisition*" of an individual to assist with information regarding the operation of the computer system or protection of the data – it is unclear what "*requisition*" means and what powers are available if this individual fails to cooperate. Section 21 HIPCAR provides for legislation to ensure assistance is provided by those who have specialist knowledge of the location of relevant evidence – this could be used as a guide – also see section 17 HIPCAR for an offence if assistance is refused without lawful excuse The national legislation should include provision to take "*a printout of output of computer data and seize or similarly secure a computer system or part of it or a computer-data storage medium*" - see definition of "*seize*" in HIPCAR section 3(16) A definition of "*requisition*" and what powers are available to ensure reasonable assistance is provided – or use section 21 HIPCAR as a guide with the offence in section 17

Procedure		
International Best Practice	**National Legislation**	**Comments**
i. a computer system or part of it and computer data stored therein; and ii. a computer-data storage medium in which computer data may be stored in the territory of the country. 2. If [law enforcement] [police] officer that is undertaking a search based on Sec. 20 (1) has grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, he shall be able to expeditiously extend the search or similar accessing to the other system. 3. A [law enforcement] [police] officer that is undertaking a search are empowered to seize or similarly secure computer data accessed according to paragraphs 1 or 2. **Section 21 HIPCAR – Assistance** Any person who is not a suspect of a crime but who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein that is the subject of a search under section 20 must permit, and assist if reasonably required and requested by the person authorized to make the search by: • providing information that enables the undertaking of measures referred to in section 20; • accessing and using a computer system or computer data storage medium to search any computer data available to or in the system; • obtaining and copying such computer data; • using equipment to make copies; and	**Article 5** The competent judicial authorities and judicial police officers acting within the framework of the Code of Criminal Procedure and in the cases provided for in Article 4 above may, **for search purposes, have access to**, Distance: (A) **a computer system or a part thereof and the computer data stored therein;** **Or (b) a computer storage system.** Where in the case provided for in paragraph (a) of this Article the authority conducting the search has reason to believe that the data sought is stored in another computer system and that such data is accessible from the original system, **It may promptly extend the search to the system in question or to a part thereof upon prior notification by the competent judicial authority.** **If it has previously been established that the data sought, accessible by means of the first system, are stored in another computer system located outside the national territory, they shall be obtained with the assistance of the competent foreign authorities in accordance with the relevant international agreements the principle of reciprocity.**	

Procedure		
International Best Practice	**National Legislation**	**Comments**
• obtaining an intelligible output from a computer system in such a format that is admissible for the purpose of legal proceedings. **Article 26 CITO - Inspecting Stored Information** 1. Every State Party shall commit itself to adopting the procedures necessary to enable its competent authorities to inspect or access: a. aan information technology or part thereof and the information stored therein or thereon. b. the storage environment or medium in or on which the information may be stored. 2. Every State Party shall commit itself to adopting the procedures necessary to enable the competent authorities to inspect or access a specific information technology or part thereof in conformity with paragraph 1 (a) if it is believed that the required information is stored in another information technology or in part thereof in its territory and such information is legally accessible or available in the first technology, the scope of inspection may be extended and the other technology accessed. **Article 27 CITO - Seizure of Stored Information** 1. Every State Party shall commit itself to adopting the procedures necessary to enable the competent authorities to seize and safeguard information technology information accessed according to Article 26, paragraph 1, of this Convention.	**The authorities in charge of the search shall be entitled to requisition any person familiar with the operation of the computer system in question or the measures applied to protect the computer data contained therein in order to assist them and to provide them with all the information necessary for the accomplishment of their mission.** **Article 6** Where the search authority discovers stored data in a computer system that is relevant to the investigation of the offense or its perpetrator, and the entry of the entire system is not necessary, the data in question as well as those necessary for their understanding, are copied on computer storage media which can be seized and sealed under the conditions provided for in the Code of Criminal Procedure. The authority conducting the search and seizure must, in any event, ensure the integrity of the data in the computer system in question. However, it may use the technical means required to format or reconstitute such data in order to render them usable for the purposes of the investigation, provided that such reconstitution or formatting of the data does not alter the content	

Procedure		
International Best Practice	**National Legislation**	**Comments**
These procedures include the authority to: a. seize and safeguard the information technology or part thereof or the storage medium for the information technology information. b. make a copy the information technology information and keep it. c. maintain the integrity of the stored information technology information. d. remove such accessed information from the information technology or prevent its access. 2. Every State Party shall commit itself to adopting the procedures necessary to enable the competent authorities to order any person who is acquainted with the functioning of the information technology or the procedures applied to protect the information technology to give the information necessary to complete the procedures mentioned in paragraphs 2 and 3 of Article 26 of this Convention.		
Article 16 BC[100] **Expedited preservation of stored computer data** 1. Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.	**No equivalent**	**Legal Analysis** This procedural power is important to ensure that data which is vulnerable to deletion or loss is preserved **Gap Analysis** **Recommendations:** This expedited power to retain BSI, metadata, transactional and stored content is essential as part of cybercrime investigations to ensure the evidence is available for search, access, seizure and review. The language of Article 16 of the BC, section 23 HIPCAR or Article 23 CITO could be used. This will also require a definition of "*subscriber information or BSI*"

[100] no equivalent in AUC

Procedure		
International Best Practice	**National Legislation**	**Comments**
2. Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 3. Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. 4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15. **Section 23 HIPCAR – Expedited Preservation** If a [law enforcement] [police] officer is satisfied that there are grounds to believe that computer data that is reasonably required for the purposes of a criminal investigation is particularly vulnerable to loss or modification, the [law enforcement] [police] officer may, by written notice given to a person in control of the computer data, require the person to ensure that the data specified in the notice be preserved for a period of up to seven (7) days as specified in the notice. The period may be extended beyond seven (7) days if, on an ex parte application, a [judge] [magistrate] authorizes an extension for a further specified period of time.		The CITO definition for subscriber information is:[101] "Any information that the service provider has concerning the subscribers to the service, except for information through which the following can be known: a. The type of communication service used, the technical requirements and the period of service. b. The identity of the subscriber, his postal or geographic address or phone number and the payment information available by virtue of the service agreement or arrangement c. Any other information on the installation site of the communication equipment by virtue of the service agreement." Consideration should be given the length of preservation that is reasonable in the circumstances and allowing for an application to extend in exigent circumstances – BC and CITO have 90 days and HIPCAR 7 days. From experience 90 days is too few in a cyber investigation and the figure should be nearer 180 days and then subject to extension.

[101] See Article 2(9) CITO

PORTADA

INDEX

Procedure		
International Best Practice	**National Legislation**	**Comments**
Article 23 CITO - Expeditious Custody of Data Stored in Information Technology 1. Every State Party shall adopt the procedures necessary to enable the competent authorities to issue orders or obtain the expeditious custody of information, including information for tracking users, that was stored on an information technology, especially if it is believed that such information could be lost or amended. 2. Every State Party shall commit itself to adopting the procedures necessary as regards paragraph 1, by means of issuing an order to a person to preserve the information technology information in his possession or under his control, in order to require him to preserve and maintain the integrity of such information for a maximum period of 90 days that may be renewed, in order to allow the competent authorities to search and investigate 3. Every State Party shall commit itself to adopting the procedures necessary to require the person responsible for safeguarding the information technology to maintain the procedures secrecy throughout the legal period stated in the domestic law.		
Article 17 BC[102] **Expedited preservation and partial disclosure of traffic data** 1. Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to	**Law No. 09-04 of 14 Chaâbane 1430 corresponding to 5 August 2009 laying down specific rules on the prevention and the fight against infringements related to information and communication technologies** **Article 2 and 10**	**Legal Analysis** This procedural power is especially important to ensure that CSPs provide IP addresses that could locate the perpetrator of a cybercrime.

[102] no equivalent in AUC

Procedure		
International Best Practice	**National Legislation**	**Comments**
a. ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and b. ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted. 2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15. **Section 23 HIPCAR – Expedited Preservation** If a [law enforcement] [police] officer is satisfied that there are grounds to believe that computer data that is reasonably required for the purposes of a criminal investigation is particularly vulnerable to loss or modification, the [law enforcement] [police] officer may, by written notice given to a person in control of the computer data, require the person to ensure that the data specified in the notice be preserved for a period of up to seven (7) days as specified in the notice. The period may be extended beyond seven (7) days if, on an ex parte application, a [judge] [magistrate] authorizes an extension for a further specified period of time.		**Gap Analysis** **Recommendation:** Article 10 of Law 09-04 imposes an obligation on communication service providers to preserve traffic data during one year. Article 2 of Law 09-04 defines "computer system", "computer data", "service providers", "traffic data", and "electronic communications" in accordance with the language of the BC and CITO.

Procedure		
International Best Practice	**National Legislation**	**Comments**
Section 24 HIPCAR – Partial Disclosure of Traffic Data If a [law enforcement] [police] officer is satisfied that data stored in a computer system is reasonably required for the purposes of a criminal investigation, the [law enforcement] [police] officer may, by written notice given to a person in control of the computer system, require the person to disclose sufficient traffic data about a specified communications to identify: a. the Internet service providers; and/or b. the path through which the communication was transmitted. **Article 24 CITO - Expeditious Custody and Partial Disclosure of Users Tracking Information** Every State Party shall commit itself to adopting the procedures necessary as regards users tracking information in order to: 1. ensure expeditious custody of users tracking information, regardless of whether such communication is transmitted by one or more service providers. 2. ensure that a sufficient amount of users tracking information is disclosed to the competent authorities of the State Party or to a person appointed by these authorities to allow the State Party to determine the service providers and the transmission path of the communications.		

Procedure		
International Best Practice	**National Legislation**	**Comments**
Article 18 BC[103] **Production Order** 1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a. a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and b. a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. 2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 3. For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a. the type of communication service used, the technical provisions taken thereto and the period of service; b. the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;	**No equivalent**	**Legal Analysis** This is an essential provision for an effective cybercrime investigation and its absence will impact upon prosecutions and international cooperation. **Gap Analysis** **Recommendation:** This investigative power is necessary to ensure CSPs in Algeria provide BSI, traffic data and stored content data. It is advisable to have a definition for "subscriber information or BSI" as different types of evidence can be produced from CSPs (i.e. BSI, traffic and content). Further this power will require individuals and others (such as corporate entities, financial institutions and other organisations) who hold data to produce it to law enforcement authorities. Article 18 BC and section 22 HIPCAR could be a guide with consistent application of definitions.

[103] no equivalent in AUC

Procedure		
International Best Practice	National Legislation	Comments
c. c.any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement. **Section 22 HIPCAR – Production Order** If a [judge] [magistrate] is satisfied on the basis of an application by a [law enforcement] [police] officer that specified computer data, or a printout or other information, is reasonably required for the purpose of a criminal investigation or criminal proceedings, the [judge] [magistrate] may order that: • a person in the territory of [enacting country] in control of a computer system produce from the system specified computer data or a printout or other intelligible output of that data; or • an Internet service provider in [enacting country] to produce information about persons who subscribe to or otherwise use the service. **Article 25 CITO - Order to Submit Information** Every State Party shall commit itself to adopting the procedures necessary to enable the competent authorities to issue orders to: 1. Any person in its territory to submit certain information in his possession which is stored on information technology or a medium for storing information. 2. Any service provider offering his services in the territory of the State Party to submit user's information related to that service which is in the possession of the service provider or under his control.		

Procedure		
International Best Practice	**National Legislation**	**Comments**
Article 21 BC[104] **Interception of content data** **Article 29 CITO - Interception of Content Information**	**Law No. 09-04 of 14 Chaâbane 1430 corresponding to 5 August 2009 laying down specific rules on the prevention and the fight against infringements related to information and communication technologies** **Article 3** In accordance with the rules laid down in the Code of Criminal Procedure and this Law and subject to the legal provisions guaranteeing the secrecy of Correspondence and communications, provision may be made for technical requirements for the protection of public order or for the purposes of investigations or judicial information in progress to **carry out electronic communications surveillance operations, Collection and recording of their content in real time,** as well as searches and seizures in a computer system.	**Legal Analysis** Article 3 allows for real-time collection of content. There are no safeguards to prevent collateral intrusion or to assess if the use of this power is necessary, proportional and reasonable. This measure must be ordered in compliance with the provisions of the Code of Criminal Procedure upon authorization by the public prosecutor or examining magistrate. This authorization must include all the elements allowing the identification of the communications to be intercepted, the offence justifying the resort to this measure, as well as its length (4 months, renewable). This measure cannot undermine professional secrecy. Article 10 of 'Act n°09-04 of 05-08-2009 on the special rules relating to the prevention and the fight against ICT-related offences' compels CSPs to provide support to the authorities responsible for judicial inquiries to collect or record content data in real-time of communications; if not, they may be prosecuted for obstruction of justice or violation of the secrecy of the investigation. Articles 1 and 2 of 'Act n°09-04 of 05-08-2009 on the special rules relating to the prevention and the fight against ICT-related offences' extend this measure to all offences committed or facilitated by computer or electronic communication systems. **Gap Analysis** **Recommendations:** The following minimum standards are suggested: 1. To ensure consistently whether the interception is justified and to prevent collateral intrusion apply the following tests: a. **Necessity**: The public prosecutor or examining magistrate should be satisfied that the proposed surveillance measure is absolutely necessary for the purposes of the investigation by demonstrating that all other means have either been exhausted or are inapplicable.

[104] no equivalent in AUC

Procedure		
International Best Practice	**National Legislation**	**Comments**
		b. **Reasonable**: The public prosecutor or examining magistrate should be satisfied the surveillance measure is the least intrusive one for the purpose of collecting the targeted information c. **Proportionality:** When invading personal privacy, the public prosecutor or examining magistrate should be satisfied the surveillance is proportionate to the seriousness of the crime – this includes consideration of collateral intrusion and minimizing harm on third parties
Article 20 BC[105] **Real-time collection of traffic data** 1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a. collect or record through the application of technical means on the territory of that Party, and b. compel a service provider, within its existing technical capability: i. to collect or record through the application of technical means on the territory of that Party; or ii. to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.	**Law No. 09-04 of 14 Chaâbane 1430 corresponding to 5 August 2009 laying down specific rules on the prevention and the fight against infringements related to information and communication technologies** **Article 3** In accordance with the rules laid down in the Code of Criminal Procedure and this Law and subject to the legal provisions guaranteeing the secrecy of Correspondence and communications, provision may be made for technical requirements for the protection of public order or for the purposes of investigations or judicial information in progress to **carry out electronic communications surveillance operations, Collection and recording of their content in real time,** as well as searches and seizures in a computer system.	**Legal Analysis** There is a specific and independent power to collect traffic data real-time as provided by the provisions of presidential decree 15-261 of 08-10-2015 on the composition, organization and functioning of the national body for the prevention and the fight against ICT-related offences (Official journal n°53 of 08-10-2015). **Gap Analysis** **Recommendations:** There should be safeguards to ensure the collection is legal, necessary, reasonable and proportionate in the circumstances. The following minimum standards are suggested: 1. **Necessity**: The public prosecutor or examining magistrate should be satisfied that the proposed surveillance measure is absolutely necessary for the purposes of the investigation by demonstrating that all other means have either been exhausted or are inapplicable. 2. **Reasonable**: The public prosecutor or examining magistrate should be satisfied the surveillance measure is the least intrusive one for the purpose of collecting the targeted information

[105] Article 31(3)(e) AUC – Note Article 28 CITO refers to expeditious collection rather than real-time collection

Procedure		
International Best Practice	National Legislation	Comments
2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory. 3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15. **Section 25 HIPCAR - Collection of Traffic Data** 1. If a [judge] [magistrate] is satisfied on the basis of [information on oath][affidavit] that there are reasonable grounds to [suspect] [believe] that traffic data associated with a specified communication is reasonably required for the purposes of a criminal investigation, the [judge] [magistrate] [may] [shall] order a person in control of such data to: • collect or record traffic data associated with a specified communication during a specified period; or • permit and assist a specified [law enforcement] [police] officer to collect or record that data.		3. **Proportionality:** When invading personal privacy, the public prosecutor or examining magistrate should be satisfied the surveillance is proportionate to the seriousness of the crime – this includes consideration of collateral intrusion and minimizing harm on third parties Article 28 CITO does not refer to real-time - only expeditious collection. Article 31(3)(e) AUC allows for real-time collection but safeguards are required. Therefore, Article 20 BC and section 25 HIPCAR should be used as a guide

Procedure		
International Best Practice	**National Legislation**	**Comments**
2. If a [judge] [magistrate] is satisfied on the basis of [information on oath] [affidavit] that there are reasonable grounds to [suspect] [believe] that traffic data is reasonably required for the purposes of a criminal investigation, the [judge] [magistrate] [may] [shall] authorize a [law enforcement] [police] officer to collect or record traffic data associated with a specified communication during a specified period through application of technical means. 3. A country may decide not to implement section 25.		
		Disclosure obligation of encryption keys With terrorists and organized criminals routinely using encrypted messaging applications[106] this may be considered a viable power to release the keys to passwords to unlock devices[107] **Gap Analysis** **Recommendation:** Unable to clarify if there were any such powers in Algeria – but such a power will allow law enforcement to compel owners to unlock devices
		Data retention obligations[108] Such a power can allow law enforcement to 1. Trace and identify the source of a communication 2. Identify the destination of a communication; 3. Identify the date, time and duration of a communication; and 4. Identify the type of communication Algeria does have such an obligation[109]

[106] Eleanor Saitta. "Can Encryption Save Us?" Nation 300, no. 24 (June 15, 2015): 16-18. Academic Search Premier, EBSCOhost (accessed February 29, 2016).

[107] For an example see section 49 Regulation of Investigatory Powers Act 2000 (UK) - http://www.legislation.gov.uk/ukpga/2000/23/section/49

[108] In 2006 the EU issued its Data Retention Directive - EU Member States had to store electronic telecommunications data for at least six months and at most 24 months for investigating, detecting and prosecuting serious crime. In 2014, the Court of Justice of the EU invalidated the Data Retention Directive, holding that it provided insufficient safeguards against interferences with the rights to privacy and data protection. In the absence of a valid EU Data Retention Directive, Member States may still provide for a data retention scheme – for national schemes see: http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention

[109] ICMEC Global Review page 18

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
Article 22 BC[110] **Jurisdiction** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: a. in its territory; or b. on board a ship flying the flag of that Party; or c. on board an aircraft registered under the laws of that Party; or d. by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. 2. Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 3. Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition. 4. This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.	**Law No. 09-04 of 14 Chaâbane 1430 corresponding to 5 August 2009 laying down specific rules on the prevention and the fight against infringements related to information and communication technologies** **Article 15**	**Legal Analysis** Without a clearly defined scope for cybercrime offences, that are international in nature, any legislation will be restricted. Pursuant to Article 15 of Law 09-04 Algerian courts are now competent to prosecute ICT-related offences committed abroad when the perpetrator is a foreigner, when they target the institutions of the Algerian State, national defence, or the national economy's strategic interests. Article 588 of the Code of criminal procedure (as amended by Ordinance 15-02 of 23-07-2015) allows Algerian courts to prosecute and judge any foreigner committing an offence (felony or misdemeanour) abroad against State security, State's fundamental interests, Algerian diplomatic and consular officers, or against an Algerian national. **Gap Analysis** **Recommendation:** If there is a conflict between jurisdictions consideration should be given to guidelines on determining the appropriate jurisdiction to try an offence – see the Eurojust Guidelines for Deciding which Jurisdiction should Prosecute (revised 2016)[111]

[110] no equivalent in AUC

[111] http://www.eurojust.europa.eu/Practitioners/operational/Documents/Operational-Guidelines-for-Deciding.pdf

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
5. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution. **Section 19 HIPCAR – Jurisdiction** This Act applies to an act done or an omission made: • in the territory of [enacting country]; or • on a ship or aircraft registered in [enacting country]; or • by a national of [enacting country] outside the jurisdiction of any country; or by a national of [enacting country] outside the territory of [enacting country], if the person's conduct would also constitute an offence under a law of the country where the offence was committed. **Article 30 CITO - Competence** 1. Every State Party shall commit itself to adopting the procedures necessary to extend its competence to any of the offences set forth in Chapter II of this Convention, if the offence is committed, partly or totally, or was realized: a. in the territory of the State Party b. on board a ship raising the flag of the State Party. c. on board a plane registered under the law of the State Party.		

International Cooperation		
International Best Practice	National Legislation	Comments
d. by a national of the State Party if the offence is punishable according to the domestic law in the location where it was committed, or if it was committed outside the jurisdiction of any State. e. if the offence affects an overriding interest of the State. 2. Every State Party shall commit itself to adopting the procedures necessary to extend the competence covering the offences set forth in Article 31, paragraph 1, of this Convention in the cases in which the alleged offender is present in the territory of that State Party and shall not extradite him to another Party according to his nationality following the extradition request. 3. If more than one State Party claim to have jurisdiction over an offence set forth in this Convention, priority shall be accorded to the request of the State whose security or interests were disrupted by the offence, followed by the State in whose territory the offence was committed, and then by the State of which the wanted person is a national. In case of similar circumstances, priority shall be accorded to the first State that requests the extradition.		

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
Article 43 CITO **Specialized Body**[112] 1. Every State Party shall guarantee, according to the basic principles of its legal system, the presence of a specialized body dedicated 24 hours a day to ensure the provision of prompt assistance for the purposes of investigation, procedures related to information technology offences or gather evidence in electronic form regarding a specific offence. Such assistance shall involve facilitating or implementing: a. provision of technical advice. b. safeguarding information based on Articles 37 and 38. c. collecting evidence, provide legal information and locate suspects. 2. In all State Parties, such a body shall be able to communicate promptly with the corresponding body in any other State Party a. If the said body, designated by a State Party, is not part of the authorities of that State Party responsible for international bilateral assistance, that body shall ensure its ability to promptly coordinate with those authorities. 3. Every State Party shall ensure the availability of capable human resources to facilitate the work of the above mentioned body.	**No equivalent**	**Legal Analysis** This is an essential mechanism for an effective cybercrime investigative capability. **Gap Analysis** **Recommendation:** This should not require legislation to implement and subject to resources should be established as a priority. Contact details should be shared for the nominated single point of contact (SPOC) nationally, central authorities internationally and INTERPOL. Consideration should also be given to drafting a Memorandum of Understanding with national agencies so that the SPOC has authority to undertake the actions required as part of an international cybercrime investigation applying national laws and treaties. This MOU will include both incoming and outgoing requests and ensure an efficient and effective process.

[112] Article 35 BC and Article 25(2) AUC

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
Article 25 BC **General principles relating to mutual assistance** 1. The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. 2. Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35. 3. Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.	**Law No. 09-04 of 14 Chaâbane 1430 corresponding to 5 August 2009 laying down specific rules on the prevention and the fight against infringements related to information and communication technologies** **Article 16** In the course of investigations or judicial inquiries into the detection of offenses within the scope of this Act and the search for their perpetrators, **the competent authorities may use international judicial assistance to Evidence in electronic form.** **In urgent cases, and subject to international conventions and the principle of reciprocity, requests for mutual legal assistance referred to in the preceding subparagraph shall be admissible if they are made by means of rapid means of communication, such as facsimile or courier Electronic means provided that these means offer sufficient security and authentication conditions.**	**Legal Analysis** Algeria ratified CITO by Presidential Decree 14-252 of 08-09-2014 Official Journal O 57 -2014 Article 32 CITO ensures that it can be used as an instrument to facilitate MLA[113] and provides for expedited preservation of stored computer data,[114] expedited preservation and partial disclosure of traffic data[115] and disclosure of stored data[116] and traffic data[117] to CITO States. Law No. 09-04 of 14 does provide for urgent requests and the sending of evidence to a Requested State by email – but it is the mechanism to allow effective international cooperation and providing the specific investigative tools for cybercrime (such as production orders and preservation) that is required **Gap Analysis** **Recommendation:** Domestic law is required for expedited preservation of stored computer data, expedited preservation and partial disclosure of traffic data and production orders. The BC, HIPCAR and CITO can be used as precedents for expedited preservation of stored computer data,[118] expedited preservation and partial disclosure of traffic data[119] disclosure of stored data[120] and expedited gathering of traffic data[121] - there also needs to be consideration of provision for real-time interception of traffic data and content[122]. Further, there needs to be a framework to cooperate on cybercrime investigations provided by multilateral conventions such as Article 27 BC and Article 32 CITO.[123]

[113] no equivalent provision in the AUC
[114] Article 29 BC and Article 37 CITO
[115] Article 30 BC and Article 38 CITO
[116] Article 31 BC and Article 39 CITO
[117] Article 33 BC and Article 41 CITO
[118] Article 29 BC, section 23 HIPCAR and Article 37 CITO
[119] Article 30 BC, sections 23 and 24 HIPCAR and Article 38 CITO
[120] Article 31 BC and Article 39 CITO
[121] Article 41 CITO
[122] Article 33 and 34 BC and sections 25 and 26 HIPCAR
[123] There are no equivalent provisions on the procedure for MLA in AUC

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
4. Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation.The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence. 5. Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws. **Article 34 CITO - Procedures for Cooperation and Mutual Assistance Requests** The provisions of paragraphs 2-9 of this Article shall apply in case no cooperation and mutual assistance treaty or convention exists on the basis of the applicable legislation between the State Parties requesting assistance and those from which assistance is requested. If such a treaty or convention exists, the mentioned paragraphs shall not apply, unless the concerned parties agree to apply them in full or in part.	**Article 17** **Requests for mutual assistance in the exchange of information or to take any interim measure shall be complied with in accordance with relevant international conventions, bilateral agreements and the principle of reciprocity.** **Article 18** The execution of the request for assistance shall be refused if it is of such a nature as to affect national sovereignty or public order. The satisfaction of requests for mutual assistance may be conditional on the confidentiality of the information provided or on the condition that they are not used for purposes other than those indicated in the request.	Consideration should be given to allowing adjudicating authorities to authorise domestic law enforcement to investigate in the State where access to a device is known. Accessibility of information is the essential criterion to initiate an investigation in cases where it is not possible to know where the data is stored (i.e. in the cloud). This could include a "mutual recognition" of court orders issued towards communication service providers in a given State, that could be served to branches of that CSPs located in other States, depending on where the data is stored.

International Cooperation		
International Best Practice	National Legislation	Comments
2 a. Every State Party shall designate a central authority responsible for sending and responding to mutual assistance requests and for their implementation and referral to the relevant authorities for implementation. b. Central authorities shall communicate directly among themselves. c. Every State Party shall, at the time of signature or deposit of the instrument of ratification, acceptance or agreement, contact the General Secretariat of the Council of Arab Interior Ministers and the Technical Secretariat of the Arab Justice Ministers and communicate to them the names and addresses of the authorities specifically designated for the purposes of this paragraph. d. The General Secretariat of the Council of Arab Interior Ministers and the Technical Secretariat of the Arab Justice Ministers shall establish and update a registry of concerned central authorities appointed by the State Parties. Every State Party shall insure that the registry's details are correct at all times 3. Mutual assistance requests in this Article shall be implemented according to procedures specified by the requesting State Party, except in the case of non-conformity with the law of the State Party from which assistance is requested. 4. The State Party from which assistance is requested may postpone taking action on the request if such action shall affect criminal investigations conducted by its authorities.		

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
5. Prior to refusing or postponing assistance, the State Party from which assistance is requested shall decide, after consulting with the requesting State Party, whether the request shall be partially fulfilled or be subject to whatever conditions it may deem necessary. 6. The State Party from which assistance is requested shall commit itself to inform the requesting State Party of the result of the implementation of the request. If the request is refused or postponed, the reasons of such refusal or postponement shall be given. The State Party from which assistance is requested shall inform the requesting State Party of the reasons that prevent the complete fulfilment of the request or the reasons for its considerable postponement. 7. The State Party requesting assistance may request the State Party from which assistance is requested to maintain the confidentiality of the nature and content of any request covered by this chapter, except in as far as necessary to implement the request. If the State Party from which assistance is requested cannot abide by this request concerning confidentiality, it shall so inform the requesting State Party which will then decide about the possibility of implementing the request.		

International Cooperation		
International Best Practice	National Legislation	Comments
8. In case of emergency, mutual assistance requests may be sent directly to the judicial authorities in the State Party from which assistance is requested from their counterparts in the requesting State Party. In such case, a copy shall be sent concurrently from the central authority in the requesting State Party to its counterpart in the State Party from which assistance is requested. a. Communications can be made and requests submitted pursuant to this paragraph through INTERPOL. b. Whenever, according to paragraph a, a request is submitted to an authority, but that authority is not competent to deal with that request, it shall refer the request to the competent authority and directly inform the requesting State Party accordingly. c. Communications and requests carried out according to this paragraph and not concerning compulsory procedures may be transmitted directly by the competent authorities in the requesting State Party to their counterpart in the State Party from which assistance is requested. d. Every State Party may, at the time of signature, ratification, acceptance or adoption, inform the General Secretariat of the Council of Arab Interior Ministers and the Technical Secretariat of the Arab Justice Ministers that requests according to this paragraph must be submitted to the central authority for reasons of efficiency.		

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
Article 26 BC[124] **Spontaneous Information** 1. A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter. 2. Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.	**No equivalent**	**Legal Analysis** This is an important procedure to assist another state to prevent a cybercrime or to investigate it. Article 18(4)-(5) UNTOC provides for the sharing of intelligence spontaneously for matters fulfilling the definition of a serious crime[125], that is transnational[126] and involves an organized crime group[127]. Without satisfying this definition an official request will need to be sent through the usual MLA channels. On the basis of the fast-moving nature of cybercriminality this is an effective way to cooperate with other states and its absence inhibits effective international collaboration. There can be informal sharing pending a MLA request through the use of a liaison judge[128] but no domestic legislative basis spontaneously sharing with another state for evidential use for all cybercrime matters. **Gap Analysis** **Recommendation:** Use UNTOC Article 18(4)-(5) as the basis to spontaneously share information (with guarantees provided about use in evidence or disclosure of sensitive information to a third party (including another state).[129] Otherwise consider legislation based on Article 33 CITO or Article 26 BC.

[124] there is no equivalent provision in the AUC

[125] Article 2(b) UNTOC ““*Serious crime” shall mean conduct constituting an offence punish- able by a maximum deprivation of liberty of at least four years or a more serious penalty*”

[126] Article 3(1) UNTOC

[127] Article 2(a) UNTOC ““*Organized criminal group” shall mean a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit*”

[128] Algeria MLA questionnaires provides an example between French and Algerian Liaison Judges

[129] See Article 33(2) CITO

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
Article 33 CITO - Circumstantial Information 1. A State Party may – within the confines of its domestic law – and without prior request, give another State information it obtained through its investigations if it considers that the disclosure of such information could help the receiving State Party in investigating offences set forth in this convention or could lead to a request for cooperation from that State Party. 2. Before giving such information, the State Party providing it may request that the confidentiality of the information be kept; if the receiving State Party cannot abide by this request, it shall so inform the State Party providing the information which will then decide about the possibility of providing the information. If the receiving State Party accepts the information on condition of confidentiality, the information shall remain between the two sides.		
Article 32 BC **Trans-border access to stored computer data with consent or where publicly available** 1. A Party may, without the authorisation of another Party: a. access publicly available (open source) stored computer data, regardless of where the data is located geographically; or	**No equivalent**	**Legal Analysis** This procedural power enables a state to secure content stored in another state in limited circumstances. Article 32.b BC and Article 40 CITO is an exception to the principle of territoriality and permits unilateral transborder access without the need for mutual legal assistance where there is consent or the information is publicly available. Examples of use of this procedural power under BC Article 32.b include: A person's e-mail may be stored in another country by a service provider, or a person may intentionally store data in another country. These persons may retrieve the data and, provided that they have the lawful authority, they may voluntarily disclose the data to law enforcement officials or permit such officials to access the data[130]

[130] BC Explanatory Report Paragraph 294

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
b. access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system. **Section 27 HIPCAR – Forensic Software** 1. If a [judge] [magistrate] is satisfied on the basis of [information on oath] [affidavit] that in an investigation concerning an offence listed in paragraph 7 herein below there are reasonable grounds to believe that essential evidence cannot be collected by applying other instruments listed in Part IV but is reasonably required for the purposes of a criminal investigation, the [judge] [magistrate] [may] [shall] on application authorize a [law enforcement] [police] officer to utilize a remote forensic software with the specific task required for the investigation and install it on the suspect's computer system in order to collect the relevant evidence. The application needs to contain the following information: a. suspect of the offence, if possible with name and address; and b. description of the targeted computer system; and c. description of the intended measure, extent and duration of the utilization; and d. reasons for the necessity of the utilization.		A suspected terrorist is lawfully arrested while his/her mailbox – possibly with evidence of a crime – is open on his/her tablet, smartphone or other device. If the suspect voluntarily consents that the police access the account and if the police are sure that the data of the mailbox is located in another state, police may access the data under Article 32.b. **Gap Analysis** **Recommendation:** This restricted power to unilaterally secure evidence is included in legislation with safeguards to ensure the consent is lawfully obtained from the user.[131] Language can be used from Article 32 BC and Article 40 CITO. Article 32.b has been heavily criticized and it may be considered that the consent of the state where the stored computer data is stored is obtained in addition to the user. Section 27 HIPCAR provides for forensic software and this may allow access to a computer in another state. There are a number of restrictions that requires the evidence cannot be obtained by other means, a judicial order is required, can only apply to certain offences and is for a restricted period (3 months). Consideration should also be given to consent of the other state where the forensic software may intrude.

[131] Consideration should be given to situations such as the non-availability of a user (e.g. death) and if consent can be obtained in another state

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
2. Within such investigation it is necessary to ensure that modifications to the computer system of the suspect are limited to those essential for the investigation and that any changes if possible can be undone after the end of the investigation. During the investigation, it is necessary to log a. the technical mean used and time and date of the application; and b. the identification of the computer system and details of the modifications undertaken within the investigation; c. any information obtained. Information obtained by the use of such software needs to be protected against any modification, unauthorized deletion and unauthorized access. 3. The duration of authorization in section 27 (1) is limited to [3 months]. If the conditions of the authorization is no longer met, the action taken are to stop immediately. 4. The authorization to install the software includes remotely accessing the suspects computer system. 5. If the installation process requires physical access to a place the requirements of section 20 need to be fulfilled. 6. If necessary a [law enforcement] [police] officer may pursuant to the order of court granted in (1) above request that the court order an internet service provider to support the installation process. 7. [List of offences].		

International Cooperation		
International Best Practice	National Legislation	Comments
8. A country may decide not to implement section 27. **Article 40 CITO - Access to Information Technology Information Across Borders** A State Party may, without obtaining an authorization from another State Party: 1. Access information technology information available to the public (open source), regardless of the geographical location of the information. 2. Access or receive – through information technology in its territory – information technology information found in the other State Party, provided it has obtained the voluntary and legal agreement of the person having the legal authority to disclose information to that State Party by means of the said information technology.		

Egypt

Egypt has ratified CITO. On 14 August 2018 Egypt adopted the Law 175/2018 on Combating Information Technology Crimes. The Anti-Cybercrime Law regulates activities online, and, according to official statements, it aims to complement the new press and media laws, which penalize, inter alia, unlicensed online activity and content violations, such as fake news.

EuroMed Justice Team endeavors to keep the information up to date and correct; however, due to the current project limitation in time and resources an analyses of the 2018 new legal provisions was not possible at this stage; some of the modification operated through this law are present within the EuroMed digital Evidence Manual.

Offences		
International Best Practice	**National Legislation**	**Comments**
Article 2 BC – Illegal Access[132] Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system. **Section 4 HIPCAR – Illegal Access** 1. A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, accesses the whole or any part of a computer system commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. .		**Legal Analysis** CITO refers to *"illicit access to, presence in or contact with"* without defining what these acts mean. BC refers to *"without right"* in Article 2 on the basis the access is unauthorized. The BC Explanatory Report confirmed the derivation of *"without right"* as, *"conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law."*[133] The Commentary sections[134] on the HIPCAR model legislation provides an explanation as to the requirement for *"without lawful excuse or justification"* as follows, *"Access to a computer system can only be prosecuted under Section 4, if it happens "without lawful excuse or justification". This requires that the offender acts without authority (whether legislative, executive, administrative, judicial, contractual or consensual) and the conduct is otherwise not covered by established legal defences, excuses, justifications or relevant principles. Access to a system permitting free and open access by the public or access to a system with the authorisation of the owner or other rights-holder is as a consequently not criminalised. Network administrators and security companies that test the protection of computer systems in order to identify potential gaps in security measures do not commit a criminal act."*

[132] Article 6 CITO and Article 29(1) AUC

[133] Paragraph 38, page 8 Explanatory Report to the Convention on Cybercrime – No.185 https://rm.coe.int/16800cce5b

[134] Page 30 Commentary Section HIPCAR Model Legislation

Offences		
International Best Practice	**National Legislation**	**Comments**
2. A country may decide not to criminalize the mere unauthorized access provided that other effective remedies are available. Furthermore, a country may require that the offence be committed by infringing security measures or with the intent of obtaining computer data or other dishonest intent **Section 5 HIPCAR – Illegal Remaining** 1. A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, remains logged in a computer system or part of a computer system or continues to use a computer system commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. 2. A country may decide not to criminalize the mere unauthorized remaining provided that other effective remedies are available. Alternatively, a country may require that the offence be committed by infringing security measures or with the intent of obtaining computer data or other dishonest intent.	**No equivalent**	Article 6 CITO refers to "*illicit access to, presence in or contact with*" without defining what these acts mean – therefore, BC and HIPCAR are to be preferred. **Gap Analysis** **Recommendation:** The national legislation could incorporate relevant language from Article 2 BC/sections 4 and 5 HIPCAR to include definitions of a *computer system* and the inclusion of programs within the definition of *data* as some data includes programs and other data does not. Further, to be consistent with international standards the legislation should refer to access "*without right*" rather than *fraudulently*. Also consider a separate offence of remaining in a computer system as per section 5 HIPCAR.

Offences		
International Best Practice	National Legislation	Comments
Article 3 BC[135] **Illegal Interception** Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system. **Section 6 HIPCAR – Illegal Interception** 1. A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, intercepts by technical means: a. any non-public transmission to, from or within a computer system; or b. electromagnetic emissions from a computer system commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. 2. A country may require that the offence be committed with a dishonest intent, or in relation to a computer system that is connected to another computer system, or by circumventing protection measures implemented to prevent access to the content of non-public transmission.	**Criminal Code No. 58/1937** **Article 309 bis** **Communications Law Act no. 10/2003** **Article 73**	**Legal Analysis** This offence is essential to prosecute transmissions of computer data to, from, or within a computer system that may be illegally intercepted to obtain information (e.g. wikileaks or Panama Papers). The Criminal Code Article 309 bis is not specific to cyber technology. Article 309bis can be used, together with Communications Law Act no. 10/2003 Articles 73b by the Public Prosecution and Economic courts for illegal computer interception. **Gap Analysis** **Recommendation:** Use the BC language in Article 3, HIPCAR section 6 as a guide - the language in Article 7 CITO is appropriate – albeit there is no definition of "information technology data"

[135] Article 29(2) AUC

Offences		
International Best Practice	**National Legislation**	**Comments**
Article 7 CITO **Illicit Interception** The deliberate unlawful interception of the movement of data by any technical means, and the disruption of transmission or reception of information technology data.		
Article 4 BC[136] **Data Interference** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm. **Section 7 HIPCAR – Illegal Data Interference** 1. A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, does any of the following acts: • damages or deteriorates computer data; or • deletes computer data; or • alters computer data; or • renders computer data meaningless, useless or ineffective; or • obstructs, interrupts or interferes with the lawful use of computer data; or • obstructs, interrupts or interferes with any person in the lawful use of computer data; or	**No equivalent**	**Legal Analysis** As above for Illicit Access there is no reference in CITO to "without right" and does not include suppression of computer data which is an element of phishing to obtain illegal access by installing a keylogger to obtain sensitive information.[137] **Gap Analysis** **Recommendation:** The absence of certain key elements related to this offence in CITO may be remedied using language from Article 4 BC or section 7 HIPCAR.

[136] Article 29(1)(e-f) AUC

[137] http://www.coe.int/en/web/cybercrime/guidance-notes

Offences		
International Best Practice	**National Legislation**	**Comments**
- denies access to computer data to any person authorized to access it; commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. **Article 8 CITO** **Offence Against the Integrity of Data** 1. Deliberate unlawful destruction, obliteration, obstruction, modification or concealment of information technology data. 2. The Party may require that, in order to criminalize acts mentioned in paragraph 1, they must cause severe damage.		
Article 5 BC[138] **System Interference** Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data. **Section 9 HIPCAR – Illegal System Interference** 1. A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification: - hinders or interferes with the functioning of a computer system; or - hinders or interferes with a person who is lawfully using or operating a computer system;	**No equivalent**	**Legal Analysis** This offence would prevent malware that interferes with the functioning of a computer – for example computer worms - a subgroup of malware (like computer viruses). They are self-replicating computer programs that harm the network by initiating multiple data-transfer processes. They can influence computer systems by hindering the smooth running of the computer system, using system resources to replicate themselves over the Internet or generating network traffic that can close down availability of certain services (such as websites). **Gap Analysis** **Recommendation:** Use the BC language in Article 5 or section 9 HIPCAR as a guide for national legislation. Also consider whether the prevention and prosecution of attacks against critical infrastructure needs a separate or aggravated offence (Section 9(2) HIPCAR) for example the functioning of a computer system may be hindered for terrorist purposes (e.g. hindering the system that stores stock exchange records can make them inaccurate, or hindering the functioning of critical infrastructure).[139]

[138] Article 29(1)(d) AUC no equivalent in CITO

[139] http://www.coe.int/en/web/cybercrime/guidance-notes

Offences		
International Best Practice	**National Legislation**	**Comments**
commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. 2. A person who intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification hinders or interferes with a computer system that is exclusively for the use of critical infrastructure operations, or in the case in which such is not exclusively for the use of critical infrastructure operations, but it is used in critical infrastructure operations and such conduct affects that use or impacts the operations of critical infrastructure the punishment shall be imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.		
Article 6 BC[140] **Misuse of Devices** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a. the production, sale, procurement for use, import, distribution or otherwise making available of: i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;	**No equivalent**	**Legal Analysis** As above for Illicit Access there is no reference to "*without right*" This offence will enable prosecution for the production, sale, procurement for use, import, distribution of access codes and other computerized data used to commit cybercrimes - for example computer systems may be accessed to facilitate a terrorist attack by interfering with a country's electrical power grid. Any offence would also have to consider those devices that have a legitimate as well as being put to criminal use ("*dual use*") – this should include the BC language of "*primarily adapted*"

[140] Article 9 CITO and Article 29(1)(h) AUC

Offences		
International Best Practice	**National Legislation**	**Comments**
ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b. the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3. Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article		**Gap Analysis** **Recommendation:** Use the BC language in Article 6 or section 10 HIPCA as a guide for national legislation. Please note that HIPCAR provides the option of listing the devices in a schedule if deemed appropriate – this could be restrictive and require updating with technological progress. The national law should provide a reasonable excuse so law enforcement can use devices for special investigation techniques – see the language at Article 6.2. BC or section 10(2) HIPCAR as a guide.

Offences		
International Best Practice	National Legislation	Comments
Section 10 HIPCAR – Illegal Devices 1. A person commits an offence if the person: a. intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, produces, sells, procures for use, imports, exports, distributes or otherwise makes available: i. a device, including a computer program, that is designed or adapted for the purpose of committing an offence defined by other provisions of Part II of this law; or ii. a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed; with the intent that it be used by any person for the purpose of committing an offence defined by other provisions of Part II of this law; or b. has an item mentioned in subparagraph (i) or (ii) in his or her possession with the intent that it be used by any person for the purpose of committing an offence defined by other provisions of part II of this law commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.		

Offences		
International Best Practice	**National Legislation**	**Comments**
2. This provision shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 is not for the purpose of committing an offence established in accordance with other provisions of Part II of this law, such as for the authorized testing or protection of a computer system. 3. A country may decide not to criminalize illegal devices or limit the criminalization to devices listed in a Schedule.		
Article 7 BC **Computer Related Forgery** Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches. **Section 11 HIPCAR – Computer-related Forgery** 1. A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification inputs, alters, deletes,	**Communications Law no. 10/2003** **Article 73** Whoever perpetrates any of the following acts during the performance of his job in the field of communications or because of it, shall be liable to a penalty of imprisonment for a period not less than three months and a fine of not less than five thousand pounds and not exceeding fifty thousand pounds, or either penalty: 1. Annunciation, publishing or recording the content of any communication message or part of it without any legal basis. 2. Hiding, changing, obstructing or altering any or part of communication message that he has received.	**Legal Analysis** Article 73 has a narrow scope if compared to International best practice, as it only criminalizes the act of computer related forgery for individuals committing this offence whilst working in the field of communications. Incorporation of BC article 7, section 11 HIPCAR or section 29(2)(b) AUC is advised to protect against this offending which could include phishing and spear phishing For example, computer data (such as the data used in electronic passports) may be input, altered, deleted, or suppressed with the result that inauthentic data is considered or acted upon for legal purposes as if it were authentic.[141] Section 11(2) HIPCAR also provides for the sending of multiple electronic email messages as an aggravated offence.

[141] http://www.coe.int/en/web/cybercrime/guidance-notes

Offences		
International Best Practice	**National Legislation**	**Comments**
or suppresses computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. 2. If the abovementioned offence is committed by sending out multiple electronic mail messages from or through computer systems, the penalty shall be imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. **Article 10 CITO** **Offence of Forgery** The use of information technology means to alter the truth of data in a manner that causes harm, with the intent of using them as true data. **Article 29(2)(b) AUC** Intentionally input, alter, delete, or suppress computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable and intelligible. A Party may require intent to defraud, of similar dishonest intent, before criminal liability attaches	3. Refraining from sending any communication message after being assigned to dispatch it. 4. Divulging without due right any information concerning communication Networks Users or their incoming or outgoing communications.	The language in Article 10 CITO has no reference to any dishonest intent and requires harm to be caused – the language in BC and HIPCAR is to be preferred as it does not require harm to be caused. BC and HIPCAR only requires that the "*inauthentic data*" data is "*considered*" **Gap Analysis** **Recommendation:** Use the BC language in Article 7, section 11 HIPCAR or 29(2)(b) AUC as a guide for national legislation

Offences		
International Best Practice	**National Legislation**	**Comments**
Article 8 BC[142] **Computer Related Fraud** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a. any input, alteration, deletion or suppression of computer data, b. any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person. **Section 12 HIPCAR – Computer-related Fraud** A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification causes a loss of property to another person by: • any input, alteration, deletion or suppression of computer data; • any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person the penalty shall be imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.	**No equivalent**	**Legal Analysis** The language in Article 11 CITO and 29(2)(d) AUC is vague with no reference to any dishonest intent and requires some form of "*harm*" (CITO) or "*benefit*" (AUC) without defining what this is **Gap Analysis** **Recommendation:** Providing definitions for "*data*" and "automated processing system" and including "*without authorization*" – the language in BC or HIPCAR for this offence is a good guide for national legislation

[142] Article 11 CITO and Article 29(2)(d) AUC

Offences		
International Best Practice	**National Legislation**	**Comments**
Article 9[143] **Content related offences (e.g. child pornography)** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a. producing child pornography for the purpose of its distribution through a computer system; b. offering or making available child pornography through a computer system; c. distributing or transmitting child pornography through a computer system; d. procuring child pornography through a computer system for oneself or for another person; e. possessing child pornography in a computer system or on a computer-data storage medium. 2. For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: a. a minor engaged in sexually explicit conduct; b. a person appearing to be a minor engaged in sexually explicit conduct; c. realistic images representing a minor engaged in sexually explicit conduct. 3. For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.	**Child Act amendment no. 126/2008** **Article 116 bis (a)** Any person importing, issuing, producing, preparing, displaying, printing, promoting, acquiring or broadcasting any pornographic materials involving children or are related to children sexual abuse ….. Notwithstanding any severer punishment stipulated in any other law, the same punishment shall apply on the following: a. Anyone using the computer, internet or animation to prepare, keep, process, display, publish, print or promote any pornographic materials or activities that are related to instigating or exploiting children in prostitution and pornography or to slandering or selling such children b. Anyone using the computer, internet or animation to instigate children to go stray, commit crimes or to carry out illegal activities or pornography, even if no crimes did occur	**Legal Analysis** This offence does not include possession or offer or making available or procuring for another person. There is no definition of "*pornographic materials*" or "*computer*" – not explicit if this also includes a computer system or a computer storage medium? This could mean that if child pornography is stored on a USB disk (or other storage medium) there is no offence. **Gap Analysis** **Recommendation:** The language in BC Article 9.2 or section 3(4) HIPCAR is a guide for the definition of child pornography Article 9.1.d and e. BC or section 13 HIPCAR is a guide for offences of procuring for oneself or another and storage on a computer system or computer storage medium.

[143] Article 29(3)(a-d) AUC

Offences		
International Best Practice	**National Legislation**	**Comments**
4. Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c. **Section 3(4) HIPCAR – definition of child pornography** 1. Child pornography means pornographic material that depicts presents or represents: a. a child engaged in sexually explicit conduct; b. a person appearing to be a child engaged in sexually explicit conduct; or c. images representing a child engaged in sexually explicit conduct; this includes, but is not limited to, any audio, visual or text pornographic material. **Section 13 HIPCAR – Child Pornography** 1. A person who, intentionally, without lawful excuse or justification: • produces child pornography for the purpose of its distribution through a computer system; • offers or makes available child pornography through a computer system; • distributes or transmits child pornography through a computer system; • procures and/or obtain child pornography through a computer system for oneself or for another person; • Possesses child pornography in a computer system or on a computer- data storage medium; or • knowingly obtains access, through information and communication technologies, to child pornography,		

Offences		
International Best Practice	**National Legislation**	**Comments**
commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. 2. It is a defense to a charge of an offence under paragraph (1) (b) to (1)(f) if the person establishes that the child pornography was a bona fide law enforcement purpose. 3. A country may not criminalize the conduct described in section 13 (1) (d)- (f).		
Article 10 BC[144] **Infringement of copyright**	**IP Protection Law no. 82/2002** **Article 181**	**Legal Analysis** This is adequately protected through national legislation
Article 11 BC[145] **Aiding and Abetting** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed. 2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.	**Criminal Code no. 58/1937** **Articles 40 and 41**	**Legal Analysis** Aiding and abetting others to commit offences is essential in order to prosecute those who may have provided assistance or encouraged cybercrimes to take place. Articles 40 and 41 of the Criminal Code are the general rules for aiding and abetting and attempt. These provisions can be applied to other substantive laws. **Gap Analysis** **Recommendation:** Whilst the Criminal Code already includes aiding and abetting and attempt, Article 11 BC and Article 19 CITO are recommended as a guide for inclusion in a domestic cybercrime law, so there is no doubt that aiding and abetting and attempt are criminalized.

[144] Article 17 CITO no equivalent in AUC

[145] Article 29(2)(f) AUC

Offences		
International Best Practice	**National Legislation**	**Comments**
Article 19 CITO - Attempt at and Participation in the Commission of Offences 1. Participation in the commission of any of the offences set forth in this chapter with the intention to commit the offence in the law of the State Party. 2. Attempt at the commission the offences set forth in Chapter II of this convention. 3. A State Party may reserve the right to not implement the second paragraph of this Article totally or partly.		
Article 12 BC[146] **Corporate liability** 1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on: a. a power of representation of the legal person; b. an authority to take decisions on behalf of the legal person; c. an authority to exercise control within the legal person.	**No equivalent**	**Legal Analysis** This provision is an essential element so that legal persons (e.g. corporate entities) acting on behalf of natural persons have criminal liability **Gap Analysis** **Recommendation:** Use the BC language in Article 12 as a guide for national legislation

[146] Article 20 CITO and Article 30(2) AUC

Offences		
International Best Practice	**National Legislation**	**Comments**
2. In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority. 3. Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative. 4. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.		
Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems **Article 3[147] – Dissemination of racist and xenophobic material through computer systems** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: distributing, or otherwise making available, racist and xenophobic material to the public through a computer system.	**Criminal Code no. 58/1937** **Article 161 bis** Any person who commits an act or abstains from an act that would discriminate between individuals or a group of people on grounds of sex, origin, language, religion or creed, shall be liable to imprisonment and a fine of not less than thirty thousand pounds and not exceeding fifty thousand pounds. And this discrimination resulted in wasting the principle of equal opportunities, social justice or general peace.	**Legal Analysis** Articles 161 bis and 76(2) do not specifically refer to the use of dissemination through computer systems, but these offences could be applied by the public prosecution if racist and xenophobic material was disseminated. The AUC Article 3(1)(e) which includes the creation of and downloading racist and xenophobic material through a computer system rather than merely disseminating or making such material available but does not include an intent or "without right" – the BC language is to be preferred.

[147] Article 29(3)(e) AUC no equivalent in CITO

Offences		
International Best Practice	**National Legislation**	**Comments**
2. A Party may reserve the right not to attach criminal liability to conduct as defined by paragraph 1 of this article, where the material, as defined in Article 2, paragraph 1, advocates, promotes or incites discrimination that is not associated with hatred or violence, provided that other effective remedies are available. 3. Notwithstanding paragraph 2 of this article, a Party may reserve the right not to apply paragraph 1 to those cases of discrimination for which, due to established principles in its national legal system concerning freedom of expression, it cannot provide for effective remedies as referred to in the said paragraph 2.	The penalty shall be imprisonment for a period of not less than three months and a fine of not less than fifty thousand pounds and not exceeding one hundred thousand pounds or one of these penalties if the crime referred to in the first paragraph of this article is committed by a public official, public employee or any person charged with public service. **Communications Law no. 10/2003** **Article 76(2)** Communication Misusage Penalties Without prejudice to the right for suitable indemnity, a penalty of confinement to prison and a fine not less than five hundred pounds and not exceeding twenty thousand pounds or either penalty shall be inflicted on whoever: 1. Uses or assists in using illegitimate means to conduct communication correspondence. 2. Premeditatedly disturbs or harasses a third party by misusing communication equipment.	**Gap Analysis** **Recommendation:** Although there are general provisions in Articles 161 bis and 76(2), it is recommended that the BC language in Article 3 Additional Protocol is used as a guide for national legislation to criminalize such behaviour through a computer system.
Additional Protocol **Article 4[148] – Racist and xenophobic motivated threat** Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:	**Criminal Code no. 58/1937** **Article 161 bis** **Communications Act No. 10/2003** **Article 76(2)**	**Legal Analysis** Articles 161 bis and 76(2) do not specifically refer to racist and xenophobic motivated threats through computer systems, but these offences could be applied by the public prosecution in such a situation

[148] Article 29(3)(f) AUC no equivalent in CITO

Offences		
International Best Practice	**National Legislation**	**Comments**
threatening, through a computer system, with the commission of a serious criminal offence as defined under its domestic law, (i) persons for the reason that they belong to a group, distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors, or (ii) a group of persons which is distinguished by any of these characteristics.		**Gap Analysis** **Recommendation:** Although there are general provisions in Articles 161 bis and 76(2), it is recommended that the BC language in Article 4 Additional Protocol is used as a guide for national legislation to criminalize such behaviour through a computer system.
Additional Protocol **Article 5[149] - Racist and xenophobic motivated insult** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: insulting publicly, through a computer system, (i) persons for the reason that they belong to a group distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors; or (ii) a group of persons which is distinguished by any of these characteristics. 2. A Party may either: a. require that the offence referred to in paragraph 1 of this article has the effect that the person or group of persons referred to in paragraph 1 is exposed to hatred, contempt or ridicule; b. reserve the right not to apply, in whole or in part, paragraph 1 of this article.	**Criminal Code no. 58/1937** **Article 161 bis** **Communications Act No. 10/2003** **Article 76(2)**	**Legal Analysis** Articles 161 bis and 76(2) do not specifically refer to racist and xenophobic motivated insults through computer systems, but these offences could be applied by the public prosecution in such a situation **Gap Analysis** **Recommendation:** Although there are general provisions in Articles 161 bis and 76(2), it is recommended that the BC language in Article 5 Additional Protocol is used as a guide for national legislation to criminalize such behaviour through a computer system.

[149] Article 29(3)(g) AUC no equivalent in CITO

Offences		
International Best Practice	**National Legislation**	**Comments**
Additional Protocol **Article 6[150] - Denial, gross minimisation, approval or justification of genocide or** **crimes against humanity** 1. Each Party shall adopt such legislative measures as may be necessary to establish the following conduct as criminal offences under its domestic law, when committed intentionally and without right: distributing or otherwise making available, through a computer system to the public, material which denies, grossly minimises, approves or justifies acts constituting genocide or crimes against humanity, as defined by international law and recognised as such by final and binding decisions of the International Military Tribunal, established by the London Agreement of 8 August 1945, or of any other international court established by relevant international instruments and whose jurisdiction is recognised by that Party. 2. 2A Party may either a. require that the denial or the gross minimisation referred to in paragraph 1 of this article is committed with the intent to incite hatred, discrimination or violence against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors, or otherwise b. reserve the right not to apply, in whole or in part, paragraph 1 of this article.	**No equivalent**	**Gap Analysis** **Recommendation:** Use the BC language in Article 6 Additional Protocol as a guide for national legislation

[150] Article 29(3)(h) AUC no equivalent in CITO

Offences		
International Best Practice	**National Legislation**	**Comments**
Additional Offences to Review		
Identity-related Crimes **Section 14 HIPCAR** A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification by using a computer system in any stage of the offence, intentionally transfers, possesses, or uses, without lawful excuse or justification, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a crime, commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.		**Legal Analysis** This offence covers the preparation phase of an identity –related crime of dishonesty **Gap Analysis** **Recommendation:** Inclusion in domestic legislation is advisable.
Disclosure of Details of an Investigation **Section 16 HIPCAR** An Internet service provider who receives an order related to a criminal investigation that explicitly stipulates that confidentiality is to be maintained or such obligation is stated by law and intentionally without lawful excuse or justification or in excess of a lawful excuse or justification discloses: • the fact that an order has been made; or • anything done under the order; or • any data collected or recorded under the order; commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.	**Criminal Code** **Articles 85(2), 189, 190 and 193**	**Legal Analysis** The HIPCAR offence sanctions data breaches and disclosure of sensitive information that could impact criminal investigations The national legislation, whilst not referring to data breaches explicitly – would criminalize breaches of investigation procedures, that should include data and sensitive information breaches.

Offences		
International Best Practice	**National Legislation**	**Comments**
Failing to Permit Assistance **Section 17 HIPCAR** 1. A person other than the suspect who intentionally fails without lawful excuse or justification or in excess of a lawful excuse or justification to permit or assist a person based on an order as specified by sections 20 to 22151 commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. 2. A country may decide not to criminalize the failure to permit assistance provided that other effective remedies are available.		**Legal Analysis** This offence relates to persons, with specific knowledge of relevant evidence, who refuse to assist. Often law enforcement will be reliant upon such persons to secure evidence in cyber investigations. A separate offence is the failure to provide passwords or access to codes to encrypted devices or data (i.e. "key to protected information") – section 53 of the UK Regulation of Investigatory Powers Act 2000 (RIPA) 152 provides for a criminal offence for persons who fail to comply with a section 49 RIPA Notice to disclose the "key" **Gap Analysis** **Recommendation:** Inclusion in domestic legislation is advisable.
Cyber Stalking **Section 18 HIPCAR** A person, who without lawful excuse or justification or in excess of a lawful excuse or justification initiates any electronic communication, with the intent to coerce, intimidate, harass, or cause substantial emotional distress to a person, using a computer system to support severe, repeated, and hostile behavior, commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.		**Legal Analysis** This offence criminalizes those who harass persons online– some jurisdictions may have non-computer related harassment offences – but this offence is recommended for those crimes committed online. **Gap Analysis** **Recommendation:** Inclusion in domestic legislation is advisable.

[151] Search and seizure, assistance and production orders
[152] http://www.legislation.gov.uk/ukpga/2000/23/section/53

Offences		
International Best Practice	**National Legislation**	**Comments**
Grooming Children Online **Dutch Criminal Code 248e** The person who proposes to arrange a meeting, by means of an automated work or by making use of a communication service, to a person of whom he knows, or should reasonably assume, that such person has not yet reached the age of sixteen, with the intention of committing indecent acts with this person or of creating an image of a sexual act in which this person is involved, will be punished with a term of imprisonment of at most two years or a fine of the fourth category, if he undertakes any action intended to realise that meeting. **Canadian Criminal Code** **Section 172.1** 1. Every person commits an offence who, by a means of telecommunication, communicates with a. a person who is, or who the accused believes is, under the age of 18 years, for the purpose of facilitating the commission of an offence under subsection 153(1), section 155, 163.1, 170 or 171 or subsection 212(1), (2), (2.1) or (4) with respect to that person; b. a person who is, or who the accused believes is, under the age of 16 years, for the purpose of facilitating the commission of an offence under section 151 or 152, subsection 160(3) or 173(2) or section 271, 272, 273 or 280 with respect to that person; or		**Legal Analysis** To prove the Dutch offence a meeting for sexual purposes is required with supporting evidence of online chat history with sexual intent; request for a meeting with evidence this was planned (i.e. date and place). The purpose of the Canadian law is to prevent grooming by predatory adults of children online. This offence does not require the sexual offence to have occurred. This means the accused does not need to have actually gone to meet the victim in person. The offence is committed before any actions are taken to commit the substantive offence. **Gap Analysis** **Recommendation:** Inclusion in domestic legislation is advisable to criminalise this preparatory behaviour before a sexual offence is committed

Offences		
International Best Practice	**National Legislation**	**Comments**
c. a person who is, or who the accused believes is, under the age of 14 years, for the purpose of facilitating the commission of an offence under section 281 with respect to that person. Punishment 2. Every person who commits an offence under subsection (1) is guilty of a. is guilty of an indictable offence and is liable to imprisonment for a term of not more than 10 years and to a minimum punishment of imprisonment for a term of one year; or b. is guilty of an offence punishable on summary conviction and is liable to imprisonment for a term of not more than 18 months and to a minimum punishment of imprisonment for a term of 90 days. Presumption re age 3. Evidence that the person referred to in paragraph (1)(a), (b) or (c) was represented to the accused as being under the age of eighteen years, sixteen years or fourteen years, as the case may be, is, in the absence of evidence to the contrary, proof that the accused believed that the person was under that age. 4. It is not a defence to a charge under paragraph (1)(a), (b) or (c) that the accused believed that the person referred to in that paragraph was at least eighteen years of age, sixteen years or fourteen years of age, as the case may be, unless the accused took reasonable steps to ascertain the age of the person.		

Procedure		
International Best Practice	**National Legislation**	**Comments**
Article 19 BC[153] **Search and seizure of stored computer data** 1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a. a computer system or part of it and computer data stored therein; and b. a computer-data storage medium in which computer data may be stored in its territory. 2. Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:	**Criminal Procedure Code no. 150/1950** **Articles 95, 206 and 206 bis** **Communications Law no. 10/2003** **Articles 19 and 64**	**Legal Analysis** The provisions in the Criminal Procedure Code and Communications Law do not refer to computers or computer systems or other computer storage mediums and are more applicable to interception (see below) This is an essential investigatory power and should refer to "gaining access" than "search." In the BC Explanatory Report, "Search" means to seek, read, inspect or review data. It includes the notion of searching for data and searching of (examining) data. The word "access" has a neutral meaning and reflects more accurately computer terminology.[154] **Gap Analysis** **Recommendation:** The national legislation could incorporate relevant language from BC and HIPCAR to include definitions of a *computer system*[155] and *computer data*[156] and refer consistently to *access* There should be a definition of "*seize*" to insure integrity and to specific procedures - section 3(16) HIPCAR

[153] Article 3 AUC

[154] Explanatory Report BC paragraph 191

[155] See Article 1.a. BC: "*any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data*" **or** section 3(5) HIPCAR: "*a device or a group of inter-connected or related devices, including the Internet, one or more of which, pursuant to a program, performs automatic processing of data or any other function.*"

[156] See Article 1.b. BC: "*any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function*" **or** section 3(6) HIPCAR: "*Computer data means any representation of facts, concepts, information (being either texts, sounds or images) machine-readable code or instructions, in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.*"

Procedure		
International Best Practice	National Legislation	Comments
a. a seize or similarly secure a computer system or part of it or a computer-data storage medium; b. b make and retain a copy of those computer data; c. maintain the integrity of the relevant stored computer data; d. render inaccessible or remove those computer data in the accessed computersystem. 4. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2. 5. The powers and procedures referred to in this article shall be subject to Articles 14 and 15. **Section 20 HIPCAR – Search and Seizure** 1. If a [judge] [magistrate] is satisfied on the basis of [information on oath] [affidavit] that there are reasonable grounds [to suspect] [to believe] that there may be in a place a thing or computer data: • that may be material as evidence in proving an offence; or • that has been acquired by a person as a result of an offence;		*"Seize includes:* • *activating any onsite computer system and computer data storage media;* • *making and retaining a copy of computer data, including by using onsite equipment;* • *maintaining the integrity of the relevant stored computer data;* • *rendering inaccessible, or removing, computer data in the accessed computer system;* • *taking a printout of output of computer data; or* • *seize or similarly secure a computer system or part of it or a computer- data storage medium."* Section 21 HIPCAR provides for legislation to ensure assistance is provided by those who have specialist knowledge of the location of relevant evidence – this could be used as a guide – also see section 17 HIPCAR for an offence if assistance is refused without lawful excuse

Procedure		
International Best Practice	National Legislation	Comments
the [judge] [magistrate] [may] [shall] issue a warrant authorizing a [law enforcement] [police] officer, with such assistance as may be necessary, to enter the place to search and seize the thing or computer data including search or similarly access: i. a computer system or part of it and computer data stored therein; and ii. a computer-data storage medium in which computer data may be stored in the territory of the country. 2. If [law enforcement] [police] officer that is undertaking a search based on Sec. 20 (1) has grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, he shall be able to expeditiously extend the search or similar accessing to the other system. 3. A [law enforcement] [police] officer that is undertaking a search are empowered to seize or similarly secure computer data accessed according to paragraphs 1 or 2. **Section 21 HIPCAR – Assistance** Any person who is not a suspect of a crime but who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein that is the subject of a search under section 20 must permit, and assist if reasonably required and requested by the person authorized to make the search by:		

Procedure		
International Best Practice	National Legislation	Comments
• providing information that enables the undertaking of measures referred to in section 20; • accessing and using a computer system or computer data storage medium to search any computer data available to or in the system; • obtaining and copying such computer data; • using equipment to make copies; and • obtaining an intelligible output from a computer system in such a format that is admissible for the purpose of legal proceedings. **Article 26 CITO - Inspecting Stored Information** 1. Every State Party shall commit itself to adopting the procedures necessary to enable its competent authorities to inspect or access: a. an information technology or part thereof and the information stored therein or thereon. b. the storage environment or medium in or on which the information may be stored. 2. Every State Party shall commit itself to adopting the procedures necessary to enable the competent authorities to inspect or access a specific information technology or part thereof in conformity with paragraph 1(a) if it is believed that the required information is stored in another information technology or in part thereof in its territory and such information is legally accessible or available in the first technology, the scope of inspection may be extended and the other technology accessed.		

Procedure		
International Best Practice	**National Legislation**	**Comments**
Article 27 CITO - Seizure of Stored Information 1. Every State Party shall commit itself to adopting the procedures necessary to enable the competent authorities to seize and safeguard information technology information accessed according to Article 26, paragraph 1, of this Convention. These procedures include the authority to: a. seize and safeguard the information technology or part thereof or the storage medium for the information technology information. b. make a copy the information technology information and keep it. c. maintain the integrity of the stored information technology information. d. remove such accessed information from the information technology or prevent its access. 2. Every State Party shall commit itself to adopting the procedures necessary to enable the competent authorities to order any person who is acquainted with the functioning of the information technology or the procedures applied to protect the information technology to give the information necessary to complete the procedures mentioned in paragraphs 2 and 3 of Article 26 of this Convention.		

Procedure		
International Best Practice	**National Legislation**	**Comments**
Article 16 BC[157] **Expedited preservation of stored computer data** 1. Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2. Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.	**No equivalent**	**Legal Analysis** This procedural power is important to ensure that data which is vulnerable to deletion or loss is preserved **Gap Analysis** **Recommendation:** This expedited power to retain BSI, metadata, transactional and stored content is essential as part of cybercrime investigations to ensure the evidence is available for search, access, seizure and review. The language of Article 16 of the BC, section 23 HIPCAR or Article 23 CITO could be used. This will also require definitions of "*computer data*",158 "*subscriber information or BSI*", "traffic data"159 and "*Communication* Service Provider"[160] To note BC and HIPCAR do not provide a definition of BSI – but CITO does for subscriber information:[161] "*Any information that the service provider has concerning the subscribers to the service, except for information through which the following can be known:* a. *The type of communication service used, the technical requirements and the period of service.* b. *The identity of the subscriber, his postal or geographic address or phone number and the payment information available by virtue of the service agreement or arrangement* c. *Any other information on the installation site of the communication equipment by virtue of the service agreement.*"

[157] no equivalent in AUC

[158] See Article 1.b. BC **or** section 3(6) HIPCAR

[159] See Article 1.d BC: "*any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service*" **or** section 3(18) HIPCAR: "*Traffic data means computer data that: a. relates to a communication by means of a computer system; and b. is generated by a computer system that is part of the chain of communication ; and c. shows the communication's origin, destination, route, time date, size, duration or the type of underlying services.*"

[160] See Article 1.c.BC: "*i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii any other entity that processes or stores computer data on behalf of such communication service or users of such service.*"

[161] See Article 2(9) CITO

Procedure		
International Best Practice	**National Legislation**	**Comments**
3. Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. 4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15. **Section 23 HIPCAR – Expedited Preservation** If a [law enforcement] [police] officer is satisfied that there are grounds to believe that computer data that is reasonably required for the purposes of a criminal investigation is particularly vulnerable to loss or modification, the [law enforcement] [police] officer may, by written notice given to a person in control of the computer data, require the person to ensure that the data specified in the notice be preserved for a period of up to seven (7) days as specified in the notice. The period may be extended beyond seven (7) days if, on an ex parte application, a [judge] [magistrate] authorizes an extension for a further specified period of time. **Article 23 CITO - Expeditious Custody of Data Stored in Information Technology** 1. Every State Party shall adopt the procedures necessary to enable the competent authorities to issue orders or obtain the expeditious custody of information, including information for tracking users, that was stored on an information technology, especially if it is believed that such information could be lost or amended.		Consideration should be given the length of preservation that is reasonable in the circumstances and allowing for an application to extend in exigent circumstances – BC and CITO have 90 days and HIPCAR 7 days. From experience 90 days is too few in a cyber investigation and the figure should be nearer 180 days and then subject to extension.

Procedure		
International Best Practice	**National Legislation**	**Comments**
2. Every State Party shall commit itself to adopting the procedures necessary as regards paragraph 1, by means of issuing an order to a person to preserve the information technology information in his possession or under his control, in order to require him to preserve and maintain the integrity of such information for a maximum period of 90 days that may be renewed, in order to allow the competent authorities to search and investigate 3. Every State Party shall commit itself to adopting the procedures necessary to require the person responsible for safeguarding the information technology to maintain the procedures secrecy throughout the legal period stated in the domestic law.		
Article 17 BC[162] **Expedited preservation and partial disclosure of traffic data** 1. Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to: a. ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and	**No equivalent**	**Legal Analysis** This procedural power is especially important to ensure that CSPs provide IP addresses that could locate the perpetrator of a cybercrime. **Gap Analysis** **Recommendation:** This expedited power alongside disclosure of traffic data should be included in legislation to enable effective investigations of cybercrime. The language of Article 17 of the BC, sections 23 and 24 HIPCAR or Article 24 CITO could be used. This will also require definitions of "*traffic data*" and "*Communication Service Provider*"[163]

[162] no equivalent in AUC

[163] See definitions above

Procedure		
International Best Practice	**National Legislation**	**Comments**
b. ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted. 2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15. **Section 23 HIPCAR – Expedited Preservation** If a [law enforcement] [police] officer is satisfied that there are grounds to believe that computer data that is reasonably required for the purposes of a criminal investigation is particularly vulnerable to loss or modification, the [law enforcement] [police] officer may, by written notice given to a person in control of the computer data, require the person to ensure that the data specified in the notice be preserved for a period of up to seven (7) days as specified in the notice. The period may be extended beyond seven (7) days if, on an ex parte application, a [judge] [magistrate] authorizes an extension for a further specified period of time.		

Procedure		
International Best Practice	**National Legislation**	**Comments**
Section 24 HIPCAR – Partial Disclosure of Traffic Data If a [law enforcement] [police] officer is satisfied that data stored in a computer system is reasonably required for the purposes of a criminal investigation, the [law enforcement] [police] officer may, by written notice given to a person in control of the computer system, require the person to disclose sufficient traffic data about a specified communication to identify: a. the Internet service providers; and/or b. the path through which the communication was transmitted. **Article 24 CITO - Expeditious Custody and Partial Disclosure of Users Tracking Information** Every State Party shall commit itself to adopting the procedures necessary as regards users tracking information in order to: 1. ensure expeditious custody of users tracking information, regardless of whether such communication is transmitted by one or more service providers. 2. ensure that a sufficient amount of users tracking information is disclosed to the competent authorities of the State Party or to a person appointed by these authorities to allow the State Party to determine the service providers and the transmission path of the communications.		

Procedure		
International Best Practice	**National Legislation**	**Comments**
Article 18 BC[164] **Production Order** 1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a. a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and b. a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. 2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 3. For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a. the type of communication service used, the technical provisions taken thereto and the period of service;	**Criminal Procedure Code no. 150/1950** **Articles 95, 206 and 206 bis** **Communications Law no. 10/2003** **Articles 19 and 64**	**Legal Analysis** This is an essential provision for an effective cybercrime investigation and its absence will impact upon prosecutions and international cooperation. The provisions in the Criminal Procedure Code and Communications Law do not refer to computers or computer systems or other computer storage mediums and are more applicable to interception (see below). **Gap Analysis** **Recommendation:** This essential power is necessary to ensure CSPs in Egypt provide BSI, traffic data and stored content data. This will also require definitions of *"computer data", "subscriber information or BSI", "traffic data"* and *"Communication Service Provider"*.[165] Article 25 CITO is a model that could be used and uses different definitions including *"information technology"*,[166] *"service provider"*[167] and *"data"*[168] – it is still advisable to have definitions for *"subscriber information or BSI", "traffic data"* as they will be different types of evidence that can be produced from CSPs. Further, this power will require individuals and others (such as corporate entities, financial institutions and other organisations) who hold data to produce it to law enforcement authorities. Article 18 BC and section 22 HIPCAR could be a guide with consistent application of definitions

[164] no equivalent in AUC

[165] See definitions above

[166] Article 2(1) CITO: "*any material or virtual means or group of interconnected means used to store, sort, arrange, retrieve, process, develop and exchange information according to commands and instructions stored therein. This includes all associated inputs and outputs, by means of wires or wirelessly, in a system or network.*"

[167] Article 2(2) CITO: "*any natural or juridical person, common or private, who provides subscribers with the services needed to communicate through information technology, or who processes or stores information on behalf of the communication service or its users.*"

[168] Article 2(3) CITO: "*all that may be stored, processed, generated and transferred by means of information technology, such as numbers, letters, symbols, etc…*"

Procedure		
International Best Practice	National Legislation	Comments
b. the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c. c.any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement. **Section 22 HIPCAR – Production Order** If a [judge] [magistrate] is satisfied on the basis of an application by a [law enforcement] [police] officer that specified computer data, or a printout or other information, is reasonably required for the purpose of a criminal investigation or criminal proceedings, the [judge] [magistrate] may order that: • a person in the territory of [enacting country] in control of a computer system produce from the system specified computer data or a printout or other intelligible output of that data; or • an Internet service provider in [enacting country] to produce information about persons who subscribe to or otherwise use the service. **Article 25 CITO - Order to Submit Information** Every State Party shall commit itself to adopting the procedures necessary to enable the competent authorities to issue orders to:		

Procedure		
International Best Practice	**National Legislation**	**Comments**
1. Any person in its territory to submit certain information in his possession which is stored on information technology or a medium for storing information. 2. Any service provider offering his services in the territory of the State Party to submit user's information related to that service which is in the possession of the service provider or under his control.		
Article 21 BC[169] **Interception of content data** 1. Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: a. collect or record through the application of technical means on the territory of that Party, and b. compel a service provider, within its existing technical capability: i. to collect or record through the application of technical means on the territory of that Party, or ii. to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system.	**Criminal Procedure Code** **Articles 95, 206 and 206 bis** **Article 95** The investigating judge may order the seizure of all letters, correspondences, newspapers, publications and packages found at post offices and all telegrams found at telegram offices and may order the surveillance of telecommunications or recording of conversations taking place in a specific place whenever deemed necessary for the revelation of the truth in a crime or misdemeanor punishable by incarceration for no less than a three-month period. In all cases, the acts of seizure, inspection, surveillance or recording shall be on the grounds of a justified warrant, for a period of time no longer than thirty days subject to renewal for another equivalent period or periods of time	**Legal Analysis** The investigative judge/or the Public prosecutor (through a judicial decree issued by a judge) can issue an order to record wired and unwired conversations in certain circumstances pursuant to articles 95, 206 and 206 bis. The Criminal Procedure Code does not refer to conversations made through the internet or computers and the issue has not been adjudicated upon by the Egyptian Court of Cassation. Mutual Legal Assistance Requests are sent to the international cooperation office at the Public Prosecution. If the Attorney General approves the request it is sent to the Department of information and documentation at the Egyptian Ministry of Interior, which proceeds on the interception request through trained police officers. These officers will prepare a report about the outcome *"without giving any details about the steps and technicalities of the interception"*. The police officers who carry out the interception of *"emails, IP addresses and social networking accounts"* must do so without infringing the privacy of other individuals. The grounds for each act of interception is written in the Criminal Procedure Code with the required conditions for issuing such a decree from the investigative judge.

[169] no equivalent in AUC

Procedure		
International Best Practice	**National Legislation**	**Comments**
2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory. 3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15. **Section 26 HIPCAR – Interception of Content Data** 1. If a [judge] [magistrate] is satisfied on the basis of [information on oath] [affidavit] that there are reasonable grounds to [suspect] [believe] that the content of electronic communications is reasonably required for the purposes of a criminal investigation, the magistrate [may] [shall]: • order an Internet service provider whose service is available in [enacting country] through application of technical means to collect or record or to permit or assist competent authorities with the collection or recording of content data associated with specified communications transmitted by means of a computer system; or	**Communications Act 10/2003** **Article 19** All entities and companies working in the telecommunication field shall provide the NTRA (National Telecommunications Regulatory Authority) with whatever requested of reports, statistics or information related to its activities except for matters related to National Security **Article 64** Telecommunication Services Operators, Providers, their employees and Users of such services shall not use any Telecommunication Services encryption equipment except after obtaining a written consent from each of the NTRA, the Armed Forces and National Security Entities, and this shall not apply to encryption equipment of radio and television broadcasting. With due consideration to inviolability of citizens private life as protected by law, each Operator and Provider shall, at his own expense, provide within the telecommunication networks licensed to him all technical potentials including equipment, systems, software and communication which enable the Armed Forces, and National Security Entities to exercise their powers within the law.The provision of the service shall synchronize in time with the availability of required technical potentials. Telecommunication Service Providers and Operators and their marketing agents shall have the right to collect accurate information and data concerning Users from individuals and various entities within the State.	**Gap Analysis** **Recommendations:** Specific provision should be made to compel CSPs in Egypt to cooperate with real-time collection of content; and safeguards should be incorporated to ensure the collection is legal, necessary, reasonable and proportionate in the circumstances. Consideration should be given to reviewing Article 29 of CITO, Article 21 BC and section 26 HIPCAR and incorporating language in national legislation

Procedure		
International Best Practice	**National Legislation**	**Comments**
• authorize a [law enforcement] [police] officer to collect or record that data through application of technical means. 2. A country may decide not to implement section 26. **Article 29 CITO - Interception of Content Information** 1. 1.Every State Party shall commit itself to adopting the legislative procedures necessary as regards a series of offences set forth in the domestic law, in order to enable the competent authorities to: a. gather or register through technical means in the territory of this State Party, or b. cooperate with and help the competent authorities to expeditiously gather and register content information of the relevant communications in its territory and which are transmitted by means of the information technology. 2. If, because of the domestic legal system, the State Party is unable to adopt the procedures set forth in paragraph 1(a), it may adopt other procedures in the form necessary to ensure the expeditious gathering and registration of content information corresponding to the relevant communications in its territory using the technical means in that territory. 3. Every State Party shall commit itself to adopting the procedures necessary to require the service provider to maintain the secrecy of any information when exercising the authority set forth in this Article.		

Procedure		
International Best Practice	National Legislation	Comments
Article 20 BC[170] **Real-time collection of traffic data** 1. 1.Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a. collect or record through the application of technical means on the territory of that Party, and b. compel a service provider, within its existing technical capability: i. to collect or record through the application of technical means on the territory of that Party; or ii. to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.	**Criminal Procedure Code** **Articles 95, 206 and 206 bis** **Communications Act 10/2003** **Article 19 and 64**	**Legal Analysis** As above for interception of content data the Criminal Procedure Code and Communications Act could be used to collect traffic data real-time. There could, however, be a lower threshold to collect real-time traffic data. There may be situations where a higher legal threshold to secure content is not made out by an applicant – but a lower threshold to secure traffic could be. For this reason, there should be a distinction between real-time collection of stored content and traffic data. There must be safeguards and requirements/procedure to compel CSPs cooperation to collect or record content data in real-time of specific communications in Egypt **Gap Analysis** Recommendations: There should be a specific power to collect traffic data real-time and provision should be made to compel CSPs in Egypt to cooperate with real-time collection of traffic data; and safeguards should be incorporated to ensure the collection is legal, necessary, reasonable and proportionate in the circumstances. The language from Article 28 CITO could be considered but this does not refer to real-time only expeditious collection. Article 31(3)(e) AUC allows for real-time collection but safeguards are required. Therefore, Article 20 BC and section 25 HIPCAR should be used as a guide for national legislation

[170] Article 31(3)(e) AUC – note Article 28 CITO refers to expeditious collection rather than real-time collection

Procedure		
International Best Practice	**National Legislation**	**Comments**
3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15. **Section 25 HIPCAR - Collection of Traffic Data** 1. If a [judge] [magistrate] is satisfied on the basis of [information on oath][affidavit] that there are reasonable grounds to [suspect] [believe] that traffic data associated with a specified communication is reasonably required for the purposes of a criminal investigation, the [judge] [magistrate] [may] [shall] order a person in control of such data to: • collect or record traffic data associated with a specified communication during a specified period; or • permit and assist a specified [law enforcement] [police] officer to collect or record that data. 2. If a [judge] [magistrate] is satisfied on the basis of [information on oath] [affidavit] that there are reasonable grounds to [suspect] [believe] that traffic data is reasonably required for the purposes of a criminal investigation, the [judge] [magistrate] [may] [shall] authorize a [law enforcement] [police] officer to collect or record traffic data associated with a specified communication during a specified period through application of technical means.		

Procedure		
International Best Practice	**National Legislation**	**Comments**
3. A country may decide not to implement section 25.		
	Communications Act no. 10/2003 **Article 64** Telecommunication Services Operators, Providers, their employees and Users of such services shall not use any Telecommunication Services encryption equipment except after obtaining a written consent from each of the NTRA, the Armed Forces and National Security Entities, and this shall not apply to encryption equipment of radio and television broadcasting. With due consideration to inviolability of citizens private life as protected by law, each Operator and Provider shall, at his own expense, provide within the telecommunication networks licensed to him all technical potentials including equipment, systems, software and communication which enable the Armed Forces, and National Security Entities to exercise their powers within the law. The provision of the service shall synchronize in time with the availability of required technical potentials. Telecommunication Service Providers and Operators and their marketing agents shall have the right to collect accurate information and data concerning Users from individuals and various entities within the State.	**Legal Analysis** This article prevents the use of encrypted equipment – such as pin locked devices The Article also allows for the provision of software to access encrypted services. It is unclear if there is any enforcement provision. **Gap Analysis** **Recommendation:** This may be considered too wide a power and unenforceable in view of the number of encrypted devices and messaging applications - a viable power to release the keys to passwords to unlock devices on a case by case basis is a UK provision[171]

[171] For an example see section 49 Regulation of Investigatory Powers Act 2000 (UK) - http://www.legislation.gov.uk/ukpga/2000/23/section/49

Procedure		
International Best Practice	**National Legislation**	**Comments**
		Data retention obligations[172] Such a power can allow law enforcement to 1. Trace and identify the source of a communication 2. Identify the destination of a communication; 3. Identify the date, time and duration of a communication; and 4. Identify the type of communication Egypt does not have such an obligation[173]

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
Article 22 BC[174] **Jurisdiction** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: a. in its territory; or b. on board a ship flying the flag of that Party; or c. c.on board an aircraft registered under the laws of that Party; or d. by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.	**No equivalent**	**Legal Analysis** Without a clearly defined scope for cybercrime offences, that are international in nature, any legislation will be restricted. **Gap Analysis** **Recommendation:** National legislation ensures jurisdiction is defined using the language of Article 22 BC, section 19 HIPCAR or Article 30 CITO. If there is a conflict between jurisdictions consideration should be given to guidelines on determining the appropriate jurisdiction to try an offence – see the Eurojust Guidelines for Deciding which Jurisdiction should Prosecute (revised 2016)[175]

[172] In 2006 the EU issued its Data Retention Directive - EU Member States had to store electronic telecommunications data for at least six months and at most 24 months for investigating, detecting and prosecuting serious crime. In 2014, the Court of Justice of the EU invalidated the Data Retention Directive, holding that it provided insufficient safeguards against interferences with the rights to privacy and data protection. In the absence of a valid EU Data Retention Directive, Member States may still provide for a data retention scheme – for national schemes see: http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention

[173] ICMEC Global Review page 25

[174] no equivalent in AUC

[175] http://www.eurojust.europa.eu/Practitioners/operational/Documents/Operational-Guidelines-for-Deciding.pdf

International Cooperation		
International Best Practice	National Legislation	Comments
2. Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 3. Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition. 4. This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. 5. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution. **Section 19 HIPCAR – Jurisdiction** This Act applies to an act done or an omission made: • in the territory of [enacting country]; or • on a ship or aircraft registered in [enacting country]; or • by a national of [enacting country] outside the jurisdiction of any country; or by a national of [enacting country] outside the territory of [enacting country], if the person's conduct would also constitute an offence under a law of the country where the offence was committed.		

International Cooperation		
International Best Practice	National Legislation	Comments
Article 30 CITO - Competence 1. Every State Party shall commit itself to adopting the procedures necessary to extend its competence to any of the offences set forth in Chapter II of this Convention, if the offence is committed, partly or totally, or was realized: a. in the territory of the State Party b. on board a ship raising the flag of the State Party. c. on board a plane registered under the law of the State Party. d. by a national of the State Party if the offence is punishable according to the domestic law in the location where it was committed, or if it was committed outside the jurisdiction of any State. e. if the offence affects an overriding interest of the State. 2. Every State Party shall commit itself to adopting the procedures necessary to extend the competence covering the offences set forth in Article 31, paragraph 1, of this Convention in the cases in which the alleged offender is present in the territory of that State Party and shall not extradite him to another Party according to his nationality following the extradition request.		

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
3. If more than one State Party claim to have jurisdiction over an offence set forth in this Convention, priority shall be accorded to the request of the State whose security or interests were disrupted by the offence, followed by the State in whose territory the offence was committed, and then by the State of which the wanted person is a national. In case of similar circumstances, priority shall be accorded to the first State that requests the extradition.		
Article 43 CITO **Specialized Body**[176] 1. Every State Party shall guarantee, according to the basic principles of its legal system, the presence of a specialized body dedicated 24 hours a day to ensure the provision of prompt assistance for the purposes of investigation, procedures related to information technology offences or gather evidence in electronic form regarding a specific offence. Such assistance shall involve facilitating or implementing: a. provision of technical advice. b. safeguarding information based on Articles 37 and 38. c. collecting evidence, provide legal information and locate suspects. 2. In all State Parties, such a body shall be able to communicate promptly with the corresponding body in any other State Party	**No equivalent**	**Legal Analysis** This is an essential mechanism for an effective cybercrime investigative capability. The Department of Computer and Network Crimes, established by the Minister of Interior's Decree no. 13507/2002 (as part of the Information and Documentation Department) has the capability to intercept emails, IP addresses and social networking accounts (without infringing the privacy of other individuals). The 24/7 Network is designed to respond immediately to international requests to preserve data **and** the collection of evidence **and** other assistance to investigate cybercrime (i.e. locate a suspect) **Gap Analysis** **Recommendation:** This should not require legislation to implement and subject to resources should be established as a priority. This may only require widening the remit, of the already established Department of Computer and Network Crimes, by appointing a 24/7 single point of contact (SPOC). Contact details should be shared for the nominated SPOC nationally, central authorities internationally and INTERPOL. Consideration should also be given to drafting a Memorandum of Understanding with national agencies so that the SPOC has authority to undertake the actions required as part of an international cybercrime investigation applying national laws and treaties. This MOU will include both incoming and outgoing requests and ensure an efficient and effective process.

[176] Article 35 BC and Article 25(2) AUC

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
a. If the said body, designated by a State Party, is not part of the authorities of that State Party responsible for international bilateral assistance, that body shall ensure its ability to promptly coordinate with those authorities. 3. Every State Party shall ensure the availability of capable human resources to facilitate the work of the above mentioned body.		
Article 25 BC **General principles relating to mutual assistance** 1. The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. 2. Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.		**Legal Analysis** Article 32 CITO ensures that it can be used as an instrument to facilitate MLA[177] and provides for expedited preservation of stored computer data,[178] expedited preservation and partial disclosure of traffic data[179] and disclosure of stored data[180] and traffic data[181] to CITO States. **Gap Analysis** **Recommendation:** It is advisable to legislate for the procedural powers in CITO nationally in order that they can be used for domestic investigations and further are reciprocal powers to use for states not a party to CITO CITO does not provide for real-time content and traffic data interception – this should be considered applying precedents in BC and HIPCAR.[182] The principle of reciprocity, however can apply for these provisions applying Articles 95, 206 and 206 bis of the Criminal Procedure Code and Articles 19 and 64 of the Communications Act.

[177] no equivalent provision in the AUC

[178] Article 29 BC and Article 37 CITO

[179] Article 30 BC and Article 38 CITO

[180] Article 31 BC and Article 39 CITO

[181] Article 33 BC and Article 41 CITO

[182] Article 33 and 34 BC and sections 25 and 26 HIPCAR

International Cooperation		
International Best Practice	National Legislation	Comments
3. Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party.The requested Party shall accept and respond to the request by any such expedited means of communication. 4. Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation.The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence. 5. Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.		Consideration should be given to allowing adjudicating authorities to authorise domestic law enforcement to investigate in the State where access to a device is known. Accessibility of information is the essential criterion to initiate an investigation in cases where it is not possible to know where the data is stored (i.e. in the cloud). This could include a "*mutual recognition*" of court orders issued towards communication service providers in a given State, that could be served to branches of that CSPs located in other States, depending on where the data is stored.

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
Article 34 CITO - Procedures for Cooperation and Mutual Assistance Requests 1. The provisions of paragraphs 2-9 of this Article shall apply in case no cooperation and mutual assistance treaty or convention exists on the basis of the applicable legislation between the State Parties requesting assistance and those from which assistance is requested. If such a treaty or convention exists, the mentioned paragraphs shall not apply, unless the concerned parties agree to apply them in full or in part. 2. a. Every State Party shall designate a central authority responsible for sending and responding to mutual assistance requests and for their implementation and referral to the relevant authorities for implementation. b. Central authorities shall communicate directly among themselves. c. Every State Party shall, at the time of signature or deposit of the instrument of ratification, acceptance or agreement, contact the General Secretariat of the Council of Arab Interior Ministers and the Technical Secretariat of the Arab Justice Ministers and communicate to them the names and addresses of the authorities specifically designated for the purposes of this paragraph.		

International Cooperation		
International Best Practice	National Legislation	Comments
d. The General Secretariat of the Council of Arab Interior Ministers and the Technical Secretariat of the Arab Justice Ministers shall establish and update a registry of concerned central authorities appointed by the State Parties. Every State Party shall insure that the registry's details are correct at all times 3. Mutual assistance requests in this Article shall be implemented according to procedures specified by the requesting State Party, except in the case of non conformity with the law of the State Party from which assistance is requested. 4. The State Party from which assistance is requested may postpone taking action on the request if such action shall affect criminal investigations conducted by its authorities. 5. Prior to refusing or postponing assistance, the State Party from which assistance is requested shall decide, after consulting with the requesting State Party, whether the request shall be partially fulfilled or be subject to whatever conditions it may deem necessary.		

International Cooperation		
International Best Practice	National Legislation	Comments
6. The State Party from which assistance is requested shall commit itself to inform the requesting State Party of the result of the implementation of the request. If the request is refused or postponed, the reasons of such refusal or postponement shall be given. The State Party from which assistance is requested shall inform the requesting State Party of the reasons that prevent the complete fulfilment of the request or the reasons for its considerable postponement. 7. The State Party requesting assistance may request the State Party from which assistance is requested to maintain the confidentiality of the nature and content of any request covered by this chapter, except in as far as necessary to implement the request. If the State Party from which assistance is requested cannot abide by this request concerning confidentiality, it shall so inform the requesting State Party which will then decide about the possibility of implementing the request. 8. a. In case of emergency, mutual assistance requests may be sent directly to the judicial authorities in the State Party from which assistance is requested from their counterparts in the requesting State Party. In such case, a copy shall be sent concurrently from the central authority in the requesting State Party to its counterpart in the State Party from which assistance is requested.		

International Cooperation		
International Best Practice	National Legislation	Comments
b. Communications can be made and requests submitted pursuant to this paragraph through INTERPOL. c. Whenever, according to paragraph a, a request is submitted to an authority, but that authority is not competent to deal with that request, it shall refer the request to the competent authority and directly inform the requesting State Party accordingly. d. Communications and requests carried out according to this paragraph and not concerning compulsory procedures may be transmitted directly by the competent authorities in the requesting State Party to their counterpart in the State Party from which assistance is requested. e. Every State Party may, at the time of signature, ratification, acceptance or adoption, inform the General Secretariat of the Council of Arab Interior Ministers and the Technical Secretariat of the Arab Justice Ministers that requests according to this paragraph must be submitted to the central authority for reasons of efficiency.		

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
Article 26 BC[183] **Spontaneous Information** 1. A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter. 2. Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.	**No equivalent**	**Legal Analysis** This is an important procedure to enable a state privy to information that will assist another state to prevent a cybercrime or to investigate it. Albeit available between CITO ratified states in CITO Article 33, Egypt has no domestic legal basis to share such information with non-CITO states unless an official request is sent through the usual MLA channels. Article 18(4)-(5) UNTOC provides for the sharing of intelligence spontaneously for matters fulfilling the definition of a serious crime[184], that is transnational[185] and involves an organized crime group[186]. Without satisfying this definition an official request will need to be sent through the usual MLA channels to non-CITO states. On the basis of the fast-moving nature of cybercriminality spontaneous sharing is an effective way to cooperate with other states and its absence inhibits effective international collaboration with non-CITO states. **Gap Analysis** **Recommendation:** Use UNTOC Article 18(4)-(5) as the basis to spontaneously share information that fulfils the scope of UNTOC (with guarantees provided about use in evidence or disclosure of sensitive information to a third party (including another state).[187] Consider legislation based on Article 33 CITO or Article 26 BC.

[183] Article 33 CITO - there is no equivalent provision in the AUC

[184] Article 2(b) UNTOC ““*Serious crime” shall mean conduct constituting an offence punish- able by a maximum deprivation of liberty of at least four years or a more serious penalty*”

[185] Article 3(1) UNTOC

[186] Article 2(a) UNTOC ““*Organized criminal group” shall mean a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit*”

[187] See Article 33(2) CITO

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
Article 33 CITO - Circumstantial Information 1. A State Party may – within the confines of its domestic law – and without prior request, give another State information it obtained through its investigations if it considers that the disclosure of such information could help the receiving State Party in investigating offences set forth in this convention or could lead to a request for cooperation from that State Party. 2. Before giving such information, the State Party providing it may request that the confidentiality of the information be kept; if the receiving State Party cannot abide by this request, it shall so inform the State Party providing the information which will then decide about the possibility of providing the information. If the receiving State Party accepts the information on condition of confidentiality, the information shall remain between the two sides.		
Article 32 BC **Trans-border access to stored computer data with consent or where publicly available** A Party may, without the authorisation of another Party: a. access publicly available (open source) stored computer data, regardless of where the data is located geographically; or b. access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.	**No equivalent**	**Legal Analysis** This procedural power enables a state to secure content stored in another state in limited circumstances. Article 32.b. BC and Article 40 CITO is an exception to the principle of territoriality and permits unilateral trans-border access without the need for mutual legal assistance where there is consent or the information is publicly available. Examples of use of this procedural power under BC Article 32.b. include: A person's e-mail may be stored in another country by a service provider, or a person may intentionally store data in another country. These persons may retrieve the data and, provided that they have the lawful authority, they may voluntarily disclose the data to law enforcement officials or permit such officials to access the data[188]

[188] Paragraph 294, page 53 BC Explanatory Report

International Cooperation		
International Best Practice	National Legislation	Comments
Section 27 HIPCAR – Forensic Software 1. If a [judge] [magistrate] is satisfied on the basis of [information on oath] [affidavit] that in an investigation concerning an offence listed in paragraph 7 herein below there are reasonable grounds to believe that essential evidence cannot be collected by applying other instruments listed in Part IV but is reasonably required for the purposes of a criminal investigation, the [judge] [magistrate] [may] [shall] on application authorize a [law enforcement] [police] officer to utilize a remote forensic software with the specific task required for the investigation and install it on the suspect's computer system in order to collect the relevant evidence. The application needs to contain the following information: a. suspect of the offence, if possible with name and address; and b. description of the targeted computer system; and c. description of the intended measure, extent and duration of the utilization; and d. reasons for the necessity of the utilization.		A suspected terrorist is lawfully arrested while his/her mailbox – possibly with evidence of a crime – is open on his/her tablet, smartphone or other device. If the suspect voluntarily consents that the police access the account and if the police are sure that the data of the mailbox is located in another state, police may access the data under Article 32.b. **Gap Analysis** **Recommendation:** This restricted power to unilaterally secure evidence is included in legislation with safeguards to ensure the consent is lawfully obtained from the user.[189] Language can be used from Article 32 BC and Article 40 CITO. Article 32b has been heavily criticized and it may be considered that the consent of the state where the stored computer data is stored is obtained in addition to the user. Section 27 HIPCAR provides for forensic software and this may allow access to a computer in another state. There are a number of restrictions that requires the evidence cannot be obtained by other means, a judicial order is required, can only apply to certain offences and is for a restricted period (3 months). Consideration should also be given to consent of the other state where the forensic software may intrude.

[189] Consideration should be given to situations such as the non-availability of a user (e.g. death) and if consent can be obtained in another state

International Cooperation		
International Best Practice	National Legislation	Comments
2. Within such investigation it is necessary to ensure that modifications to the computer system of the suspect are limited to those essential for the investigation and that any changes if possible can be undone after the end of the investigation. During the investigation, it is necessary to log the technical mean used and time and date of the application; and the identification of the computer system and details of the modifications undertaken within the investigation; any information obtained. Information obtained by the use of such software needs to be protected against any modification, unauthorized deletion and unauthorized access. 3. The duration of authorization in section 27 (1) is limited to [3 months]. If the conditions of the authorization is no longer met, the action taken are to stop immediately. 4. The authorization to install the software includes remotely accessing the suspects computer system. 5. If the installation process requires physical access to a place the requirements of section 20 need to be fulfilled. 6. If necessary a [law enforcement] [police] officer may pursuant to the order of court granted in (1) above request that the court order an internet service provider to support the installation process. 7. [List of offences]. 8. A country may decide not to implement section 27.		

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
Article 40 CITO - Access to Information Technology Information Across Borders A State Party may, without obtaining an authorization from another State Party: 1. Access information technology information available to the public (open source), regardless of the geographical location of the information. 2. Access or receive – through information technology in its territory – information technology information found in the other State Party, provided it has obtained the voluntary and legal agreement of the person having the legal authority to disclose information to that State Party by means of the said information technology.		

Israel

Israel deposited the instrument of accession to the Budapest Convention on 9 May 2016.

Offences		
International Best Practice	**National Legislation**	**Comments**
Article 2 BC – Illegal access Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.	**Computers Law 1995** **Section 4** A person who unlawfully penetrates computer material located in a computer, shall be liable to imprisonment for a period of three years; for this purpose, "penetration into computer material" - penetration by means of communication or connection with a computer, or by operating it, but excluding penetration into computer material which constitutes eavesdropping under the Eavesdropping Law, 5729 – 1979. **Section 5** A person who performs an act prohibited under Section 4, in order to commit an offense under any law, excluding this Law, shall be liable to imprisonment for a period of five years.	**Legal Analysis** The BC refers to *"without right"* Section 4 of the national legislation refers to *"unlawfully"* penetrating of *"computer material"* and only criminalizes the access rather than the securing of any *"computer material"* The activity of obtaining information would constitute an offence, such as the offense of violating privacy, fraudulently or deceitfully obtaining matter or theft Israeli law only requires an intent to commit a serious offence (i.e aggravated circumstances). Unlawful penetration contrary to section 4 is a standalone offence. This is consistent with the BC, which does not require proof that the illegal access was to commit another offence.
Article 3 BC - **Illegal Interception**	**Wiretapping Law** **Section 2**	**Legal Analysis** Section 2 of the Wiretapping Law provides for this criminal offence.An offence of illegal interception is essential to prosecute non-public transmissions of computer data to, from, or within a computer system that may be illegally intercepted to obtain information about a person's location (e.g. to target that person).[190]

[190] http://www.coe.int/en/web/cybercrime/guidance-notes

Offences		
International Best Practice	**National Legislation**	**Comments**
Article 4 BC - **Data Interference**	**Computers Law 1995** **Sections 2 and 6** 1. A person who unlawfully does one of the following, shall be liable to imprisonment for a period of three years: a. … b. Deletes computer material, alters it, disrupts it in any other way or interferes with its use. 2. (a) A person who composes a software program in a manner that enables it to cause damage to or disruption of a non-specific computer or computer material, in order to unlawfully cause damage to or disruption of a computer or computer material, whether specific or non-specific, b. A person who transfers software program to another, or who infiltrates another's computer with, a software program that is capable of causing damage or disruption as aforesaid in Subsection (a), in order to unlawfully cause the aforesaid damage or disruption, shall be liable to imprisonment for a period of five years.	**Legal Analysis** The BC refers to *"without right"* and the national legislation to **"***unlawfully"* on the basis the access is unauthorized. The national offence refers at section 2(2) to deleting *"computer material"* There is no requirement to show deletion caused disruption or damage.[191] The section 6 offence would include the creation of botnets, that damage, delete, deteriorate, alter or suppress If there was any deletion or "*suppression of data*" as specified in the BC Article 4, a section 2 offence would be relevant.

[191] In the matter of the State of Israel V's Refaeli Oded, Mr. Refaeli was accused of performing a computer intrusion from an external computer to his previous employer's computer and deleted any evidence. The Court held that the correct and reasonable interpretation of section 2(2) of the Computer Act is that any deletion and/or transformation of computer materials are forbidden by the Computer Act and there is no need to prove that the deletion caused any damage or disruption.

Offences		
International Best Practice	**National Legislation**	**Comments**
Article 5 BC - **System Interference**	**Computers Law 1995** **Section 2** A person who unlawfully does one of the following, shall be liable to imprisonment for a period of three years: 1. Disrupts the proper operation of a computer or interferes with its use;	**Legal Analysis** The Computers Law refers to disrupting the *"operation of a computer"* at section 2(1) **Gap Analysis** **Recommendation:** Consider whether the prevention and prosecution of attacks against critical infrastructure needs a separate or aggravated offence for example the functioning of a computer system may be hindered for terrorist purposes (e.g. hindering the system that stores stock exchange records can make them inaccurate, or hindering the functioning of critical infrastructure).[192]
Article 6 BC - **Misuse of Devices**	**Computers Law 1995** **Section 6** a. A person who composes a software program in a manner that enables it to cause damage to or disruption of a non-specific computer or computer material, in order to unlawfully cause damage to or disruption of a computer or computer material, whether specific or non-specific, ….. b. A person who transfers software program to another, or who infiltrates another's computer with, a software program that is capable of causing damage or disruption as aforesaid in Subsection (a), in order to unlawfully cause the aforesaid damage or disruption….	**Legal Analysis** Section 6 criminalizes the production and transmission of a software program to infiltrate, cause damage or disruption. Transfer in section 6(b) would include sale of such software programmes (for example Trojans) in 6(b) and (c). Israel lodged a reservation re procurement for use and import and possession of distribution of access codes and other computerized data used to commit cybercrimes when it signed the BC. Any offence would also have to consider those devices that have a legitimate as well as being put to criminal use ("dual use") – the legislation is clear that any software program that is used to *"unlawfully cause damage to or disruption of a computer or computer material"* so adequately incorporates dual use. *"Infiltrate"* is used in section 6(b) and whilst this could mean illegal access this should be clarified Article 6.2 of the BC states that there is no need to interpret the Article as imposing criminal liability when the actions had been carried out other than for committing an offense, such as authorized protection inspections or by the Police. Under Israeli law a condition for the formation of an offence is that the action had been carried out illegally, therefore it is clear that enforcement authorities acting legally will not be criminalized, and as such do not require exemption

[192] http://www.coe.int/en/web/cybercrime/guidance-notes

Offences		
International Best Practice	**National Legislation**	**Comments**
		Gap Analysis **Recommendation:** Include a definintion of *"infiltrate"* in the Computers Law so there is clarity regarding its meaning
Article 7 BC - **Computer related forgery** Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.	**Computers Law 1995** **Section 3** a. A person who does one of the following shall be liable to imprisonment for a period of five years: 1. Transfers to another person or stores in a computer false information or performs an action with respect to information so it would result in the production of false information or false output; 2. Writes software program, transfers software program to another person or stores software program in a computer, so it would result in the production of false information or false output, or operates a computer while using software program as aforesaid. b. In this section, "*false information*" and "false output" - information or output that can mislead, pursuant to the objectives of their use.	**Legal Analysis** Article 7 covers data which is the equivalent of a public or private document. The unauthorised *"input"* of correct or incorrect data brings about a situation that corresponds to the making of a false document. Subsequent alterations (modifications, variations, partial changes), deletions (removal of data from a data medium) and suppression (holding back, concealment of data) correspond in general to the falsification of a genuine document. The section 3 offence would encapsulate computer related forgery that results in *"false information" or "false output".* The sending of a forged document or alteration of data (such as those used in phishing) would be sufficient for a conviction. A forgery offence in Article 7 BC requires an intent that inauthentic data is considered authentic. Section 3 does not require any such intent – the intent included in Article 7 BC was at the discretion of parties and is not a specific requirement. Section 6, re the production and transmission of a software program to infiltrate, cause damage or disruption, could be used for those who write or send a forged program, but requires proof of disruption or damage

Offences		
International Best Practice	**National Legislation**	**Comments**
Article 8 BC - **Computer related fraud** Each Party shall adopt suchlegislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: any input, alteration, deletion or suppression of computer data,any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person. **Section 12 HIPCAR – Computer-related Fraud** A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification causes a loss of property to another person by: a. any input, alteration, deletion or suppression of computer data; b. any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person the penalty shall be imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both	**Computers Law 1995** **Section 3**	**Legal Analysis** The aim of Article 8 BC is to criminalise any undue manipulation in the course of data processing with the intention to affect an illegal transfer of property. The Article 8 BC offence must be committed *"without right"*, and an economic benefit obtained as a result.This is to prevent criminalisation of legitimate common commercial practices. For example, activities carried out pursuant to a valid contract between the affected persons are with right (e.g. disabling a web site as entitled pursuant to the terms of the contract).[193] The Article 8 BC offence has to be committed *"intentionally"*. The general intent element refers to the computer manipulation or interference causing loss of property to another.The offence also requires a specific fraudulent or other dishonest intent to gain an economic or other benefit for oneself or another.Thus, for example, commercial practices with respect to market competition that may cause an economic detriment to a person and benefit to another, but are not carried out with fraudulent or dishonest intent, are not meant to be included in the offence established by this article. For example, the use of information gathering programs to comparison shop on the Internet (*"bots"*), even if not authorised by a site visited by the *"bot"* is not intended to be criminalised.[194] Section 3 doesn't require a false misrepresentation or dishonest intent. Section 6 could be used for those who write or send a program, but requires proof of disruption or damage **Gap Analysis** **Recommendation:** A specific computer related fraud offence is included in the Computers Law 1995 to ensure any such offence is committed *"without right"* and intentionally – using Article 8 BC or section 12 HIPCAR.

[193] Paragraph 89, page 15 BC Explanatory Report
[194] Paragraph 90, page 15 BC Explanatory Report

Offences		
International Best Practice	**National Legislation**	**Comments**
Article 9 BC - **Content related offences (e.g. child pornography)**	**Penal Code** **Section 214**	**Legal Analysis** Section 214 of the Penal Code relates to obscenity publications The term *"indecent material including the image of a minor"* is the Israeli term for *"child pornography"*. - Section 214(b)
Article 10 BC - **Infringement of copyright**	**The Agreement** on Trade-Related Aspects of Intellectual Property Rights **(TRIPS) AgreementAgreement**	As a party to the TRIPS Agreement Israel has ensured that it has criminal liability consistent with its obligations
Article 11 BC **Aiding and Abetting** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed. 2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.	**Penal Code** **Section 25** **Section 31** **Section 32**	**Legal Analysis** Aiding and abetting others to commit offences is essential in order to prosecute those who may have provided assistance or encouraged cybercrimes to take place. Sections 31 and 32 under the Penal Code include aiding and abetting. In addition, section 25 to the Penal Code defines an attempt to commit an offence
Article 12 BC - **Corporate liability** 1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:	**Penal Code** **Section 23**	**Legal Analysis** Section 23 under the Penal Code refers to criminal liability of a corporation, as well as possible civil liability (breach of statutory duty or negligence).

Offences		
International Best Practice	**National Legislation**	**Comments**
a. a power of representation of the legal person; b. an authority to take decisions on behalf of the legal person; c. an authority to exercise control within the legal person. 2. In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority. 3. Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative. 4. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.		
Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems **Article 3 – Dissemination of racist and xenophobic material through computer systems** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: distributing, or otherwise making available, racist and xenophobic material to the public through a computer system.	**No equivalent**	**Legal Analysis** There is no similar offence in Israeli law - Please note that Israel has not signed the Additional Protocol and there is no requirement to implement this Article **Gap Analysis** **Recommendation:** Use the BC language in Article 3 Additional Protocol as a guide for national legislation if required

Offences		
International Best Practice	**National Legislation**	**Comments**
2. A Party may reserve the right not to attach criminal liability to conduct as defined by paragraph 1 of this article, where the material, as defined in Article 2, paragraph 1, advocates, promotes or incites discrimination that is not associated with hatred or violence, provided that other effective remedies are available. 3. Notwithstanding paragraph 2 of this article, a Party may reserve the right not to apply paragraph 1 to those cases of discrimination for which, due to established principles in its national legal system concerning freedom of expression, it cannot provide for effective remedies as referred to in the said paragraph 2.		
Additional Protocol **Article 4 – Racist and xenophobic motivated threat** Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: threatening, through a computer system, with the commission of a serious criminal offence as defined under its domestic law, (i) persons for the reason that they belong to a group, distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors, or (ii) a group of persons which is distinguished by any of these characteristics.	**Penal Code** **Section 144(b)** **Section 192**	**Legal Analysis** Threats in general, are prohibited pursuant to section 192 under the Penal Code, this includes racial threats and non-racial. Section 144f(b) under the Penal Code (hate crime) constitutes as aggravated circumstances, which doubles the maximum punishment set for the offence to six years of imprisonment.

Offences

International Best Practice	National Legislation	Comments
Additional Protocol **Article 5 - Racist and xenophobic motivated insult** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: insulting publicly, through a computer system, (i) persons for the reason that they belong to a group distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors; or (ii) a group of persons which is distinguished by any of these characteristics. 2. A Party may either: a. require that the offence referred to in paragraph 1 of this article has the effect that the person or group of persons referred to in paragraph 1 is exposed to hatred, contempt or ridicule; or b. reserve the right not to apply, in whole or in part, paragraph 1 of this article.	**No equivalent**	**Legal Analysis** There is no offence in Israeli law - Please note that Israel has not signed the Additional Protocol and there is no requirement to implement this Article **Gap Analysis** **Recommendation:** Use the BC language in Article 5 Additional Protocol as a guide for national legislation if required.
Additional Protocol **Article 6 - Denial, gross minimisation, approval or justification of genocide or crimes against humanity** Each Party shall adopt such legislative measures as may be necessary to establish the following conduct as criminal offences under its domestic law, when committed intentionally and without right: distributing or otherwise making available, through a computer system to the public, material which denies, grossly minimises, approves or justifies acts constituting,	**No equivalent**	**Legal Analysis** Israeli law does not include a prohibition on the denial of genocide or justification of it (as long it is not considered incitement to violence) - Please note that Israel has not signed the Additional Protocol and there is no requirement to implement this Article **Gap Analysis** **Recommendation:** *Use* the BC language in Article 6 Additional Protocol as a guide for national legislation if required.

Offences		
International Best Practice	**National Legislation**	**Comments**
genocide or crimes against humanity, as defined by international law and recognised as such by final and binding decisions of the International Military Tribunal, established by the London Agreement of 8 August 1945, or of any other international court established by relevant international instruments and whose jurisdiction is recognised by that Party. 3. A Party may either a. require that the denial or the gross minimisation referred to in paragraph 1 of this article is committed with the intent to incite hatred, discrimination or violence against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors, or otherwise b. reserve the right not to apply, in whole or in part, paragraph 1 of this article.		
Additional Offences to Review		
Identity-related Crimes **Section 14 HIPCAR** A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification by using a computer system in any stage of the offence, intentionally transfers, possesses, or uses, without lawful excuse or justification, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a crime, commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.	**Penal Code** **Section 441** **Computers Law** **Section 3**	**Legal Analysis** This offence covers the preparation phase of an identity –related crime of dishonesty. Such acts may constitute an offence of impersonation (section 441 under the Penal Code) and false information (Section 3 under the Computers Law)

Offences		
International Best Practice	**National Legislation**	**Comments**
Disclosure of Details of an Investigation **Section 16 HIPCAR** An Internet service provider who receives an order related to a criminal investigation that explicitly stipulates that confidentiality is to be maintained or such obligation is stated by law and intentionally without lawful excuse or justification or in excess of a lawful excuse or justification discloses: • the fact that an order has been made; or • anything done under the order; or • any data collected or recorded under the order; commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.	**Criminal Procedure (Enforcement** **Powers - Communications Data) 5768 - 2007** **Section 5 and 11(a)** **Penal Code** **Section 287**	**Legal Analysis** This offence sanctions data breaches and disclosure of sensitive information that could impact criminal investigations. Section 5 together with section 11(a) under the Criminal Procedure (Enforcement Powers - Communications Data), 5768 - 2007 provides for the criminal liability of an Internet provider that discovers it has been issued an order and acts in violation of the order's instructions under the Communications Data Law. In respect of other orders, Israeli law includes the offence of violation of a legal instruction (section 287 under the Penal Code).
Failing to Permit Assistance **Section 17 HIPCAR** 1. A person other than the suspect who intentionally fails without lawful excuse or justification or in excess of a lawful excuse or justification to permit or assist a person based on an order as specified by sections 20 to 22[195] commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. 2. A country may decide not to criminalize the failure to permit assistance provided that other effective remedies are available.	**Penal Code** **Contempt of Court Ordinance**	**Legal Analysis** This offence relates to persons, with specific knowledge of relevant evidence, who refuse to assist. Often law enforcement will be reliant upon such persons to secure evidence in cyber investigations. A separate offence is the failure to provide passwords or access to codes to encrypted devices or data (i.e. "*key to protected information*") – section 53 of the UK Regulation of Investigatory Powers Act 2000 (RIPA)[196] provides for a criminal offence for persons who fail to comply with a section 49 RIPA Notice to disclose the "*key*" Breach of a legal instruction is an offence under Israeli Penal Code or pursuant to the Israeli Contempt of Court Ordinance. This include a failure to comply with an instruction to provide a password or pin code.

[195] Search and seizure, assistance and production orders

[196] http://www.legislation.gov.uk/ukpga/2000/23/section/53

Offences		
International Best Practice	**National Legislation**	**Comments**
Cyber Stalking **Section 18 HIPCAR** A person, who without lawful excuse or justification or in excess of a lawful excuse or justification initiates any electronic communication, with the intent to coerce, intimidate, harass, or cause substantial emotional distress to a person, using a computer system to support severe, repeated, and hostile behavior, commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.	**Communication Law (Bezeq and Transmission)** **Section 30**	**Legal Analysis** The offence contrary to section 30 of the Communication Law criminalizes those who harass persons online.
Grooming Children Online **Dutch Criminal Code 248e** The person who proposes to arrange a meeting, by means of an automated work or by making use of a communication service, to a person of whom he knows, or should reasonably assume, that such person has not yet reached the age of sixteen, with the intention of committing indecent acts with this person or of creating an image of a sexual act in which this person is involved, will be punished with a term of imprisonment of at most two years or a fine of the fourth category, if he undertakes any action intended to realise that meeting. **Canadian Criminal Code** **Section 172.1** 1. Every person commits an offence who, by a means of telecommunication, communicates with		**Legal Analysis** To prove the Dutch offence a meeting for sexual purposes is required with supporting evidence of online chat history with sexual intent; request for a meeting with evidence this was planned (i.e. date and place). The purpose of the Canadian law is to prevent grooming by predatory adults of children online. This offence does not require the sexual offence to have occurred. This means the accused does not need to have actually gone to meet the victim in person. The offence is committed before any actions are taken to commit the substantive offence. **Gap Analysis** **Recommendation:** Inclusion in domestic legislation is advisable to criminalise this preparatory behaviour before a sexual offence is committed

Offences		
International Best Practice	**National Legislation**	**Comments**
a. a person who is, or who the accused believes is, under the age of 18 years, for the purpose of facilitating the commission of an offence under subsection 153(1), section 155, 163.1, 170 or 171 or subsection 212(1), (2), (2.1) or (4) with respect to that person; b. a person who is, or who the accused believes is, under the age of 16 years, for the purpose of facilitating the commission of an offence under section 151 or 152, subsection 160(3) or 173(2) or section 271, 272, 273 or 280 with respect to that person; or c. a person who is, or who the accused believes is, under the age of 14 years, for the purpose of facilitating the commission of an offence under section 281 with respect to that person. Punishment 2. Every person who commits an offence under subsection (1) is guilty of a. is guilty of an indictable offence and is liable to imprisonment for a term of not more than 10 years and to a minimum punishment of imprisonment for a term of one year; or b. is guilty of an offence punishable on summary conviction and is liable to imprisonment for a term of not more than 18 months and to a minimum punishment of imprisonment for a term of 90 days.		

Offences		
International Best Practice	**National Legislation**	**Comments**
Presumption re age 3. Evidence that the person referred to in paragraph (1)(a), (b) or (c) was represented to the accused as being under the age of eighteen years, sixteen years or fourteen years, as the case may be, is, in the absence of evidence to the contrary, proof that the accused believed that the person was under that age. No defence 4. It is not a defence to a charge under paragraph (1)(a), (b) or (c) that the accused believed that the person referred to in that paragraph was at least eighteen years of age, sixteen years or fourteen years of age, as the case may be, unless the accused took reasonable steps to ascertain the age of the person.		

Procedure		
International Best Practice	**National Legislation**	**Comments**
Article 19 BC - **Search and seizure of stored computer data** 1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a. a computer system or part of it and computer data stored therein; and b. a computer-data storage medium in which computer data may be stored in its territory.	**Criminal Procedure (Arrest and Search) Ordinance [New Version], 5729 – 1969** **Section 23A** **Penetration of computer material** **Section 32** **Power to seize objects**	**Legal Analysis** Section 23A allows for the *"penetration of a computer material - within its meaning in section 4 of the Computers Law 5755-1995"* Section 1 of the Computers Law defines *"penetration of a computer material"*. Section 32 provides that a policeman may seize an *"object"*, that includes *"computer material"* Albeit, section 32 refers to a trained official, it does not refer to copying, preserving original data content, ensuring the integrity of any evidence seized or rendering the data inaccessible to prevent any further offending. However, copying and preservation is done as a matter of routine by the Israel Police, and the information is kept.

Procedure		
International Best Practice	National Legislation	Comments
2. Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2.These measures shall include the power to: a. seize or similarly secure a computer system or part of it or a computer-data storage medium; b. make and retain a copy of those computer data; c. maintain the integrity of the relevant stored computer data; d. render inaccessible or remove those computer data in the accessed computersystem.		

Procedure		
International Best Practice	National Legislation	Comments
4. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2. 5. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.		

Procedure		
International Best Practice	**National Legislation**	**Comments**
Article 16 BC **Expedited preservation of stored computer data** 1. Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2. Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 3. Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. 4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Criminal Procedure Law (Communication's Data) (2007)** **Article 3 and 4** **Criminal Procedure Ordinance (Arrest and Search) (1969)** **Article 43**	**Legal Analysis** This procedural power is important to ensure that data which is vulnerable to deletion or loss is preserved Article 3 and 4, of the Criminal Procedure Law (Communications Data) (2007) provides for preservation of communication's data. Article 43 of the Criminal Procedure Ordinance (Arrest and Search) (1969) provide for preservation of any other computer data.

Procedure		
International Best Practice	**National Legislation**	**Comments**
Article 17 BC **Expedited preservation and partial disclosure of traffic data** 1. Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to: a. ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and b. ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted. 2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Communications Law** **Article 13(b)(2)** **Criminal Procedure Law (Communications Data) 2007**	**Legal Analysis** This procedural power is especially important to ensure that CSPs provide IP addresses that could locate the perpetrator of a cybercrime. Article 13(b)(2) of the Communications Law (1982), alongside specific guidelines of the Israeli Police, allows for partial disclosure of traffic data with judicial oversight pursuant to Articles 3 and 4 of the Criminal Procedure Law (Communications Data) (2007).
Article 18 BC **Production Order** 1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a. a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and	**Criminal Procedure (Enforcement Powers - Communications Data) 5768 - 2007** **Article 3 and 4** **Criminal Procedure Ordinance (Arrest and Search) (1969)** **Article 43**	**Legal Analysis** Articles 3 and 4 of the Criminal Procedure (Enforcement Powers - Communications Data) 5768 - 2007 provides for preservation of communication data. Article 43 of the Criminal Procedure Ordinance (Arrest and Search) (1969) provides for preservation of any other computer data.

Procedure		
International Best Practice	National Legislation	Comments
b. a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. 2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 3. For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a. the type of communication service used, the technical provisions taken thereto and the period of service; b. the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c. any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.		

Procedure		
International Best Practice	**National Legislation**	**Comments**
Article 21 BC - **Interception of content data** 1. Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: a. collect or record through the application of technical means on the territory of that Party, and b. compel a service provider, within its existing technical capability: i. to collect or record through the application of technical means on the territory of that Party, or ii. to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.		**Legal Analysis**[197] The Wiretapping Law, 1979 permits monitoring, recording or copying of conversations of others without the consent of any of the participants subject to protection of privacy. The Wiretapping Law 1979 was amended in 1995 to allow the balancing of interests and rights, with the right to privacy through judicially authorized wiretapping. The 1981 Law Protecting Privacy defines lawful and unlawful limitations to privacy. that include: reasonable limitation of privacy by a security authority in completion of its duties (i.e. police investigations). The right to privacy will have priority and unlawfully obtained evidence will not be admitted into evidence; unless in exceptional cases for maintaining the rule of law.[198] A Conversation is defined in the law as speech, telephone, mobile phone, radio waves, fax, telex, teleprinter, **and communication between computers.** The measure may be used when necessary for the discovery, investigation, or prevention of an offence in the category of felony (offences punishable by at least 3 years of imprisonment), or for the discovery or capture of criminals who have committed such offences, or in an investigation for purposes of confiscating property connected to these offences. The Legal Assistance between States Law, 1998, allows a requesting state to request interception if it is necessary in connection with a criminal matter in the requesting state, regarding one of the following: 1. An offence which under the laws of the requesting state is punishable by over 3 years of imprisonment. 2. An offence which if committed in Israel would have provided grounds for permitting wiretapping. 3. For purposes of confiscation The President of the District Court or his authorized deputy is the body authorized to permit wiretapping by a warrant.

[197] EuroMed Fiche 2014 pages 82-84

[198] HCJ 3815/90 Gilat v. Minister of Police and Others; 3816 Yefet and Others v. Minister of Police and others

Procedure		
International Best Practice	**National Legislation**	**Comments**
3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.	**Wiretapping Law 1979**	An application for a warrant as stated shall be filed by a police officer with a rank of commander (Nitzav Mishneh) and above. The application shall be filed using a standard form, and shall specify, inter alia, the factual foundation upon which the application is based, the reasons for the application, and the details of the action requested. The application shall be heard ex parte. The permit in the warrant shall be given after the competent body has considered the severity of the infringement of privacy, and the measure is necessary for the discovery, investigation, and prevention of an offence in the category of felony (offences punishable by at least 3 years of imprisonment), or for the discovery or capture of criminals who have committed such crimes, or in an investigation for purposes of confiscating property connected to such offences. The permit shall specify the identity of the person, the identity of the line or the installation, place or type of conversations and the methods of wiretapping. The duration of the permit shall be for a period of up to three months, and it may be extended from time to time. Once a month, the Police Commissioner will report on the permits issued. The Police Commissioner is authorized to issue an urgent permit for 48 hours when there is no time to obtain a permit and it is necessary for the prevention of a felony and the discovery of its perpetrator. The Commissioner shall report to the Attorney General immediately upon issuing the permit and the latter has the authority to revoke it. By law, incoming requests for legal assistance in criminal matters may be received by the Directorate of Courts, the Director of the Department of International Affairs of the State Attorney's Office or the Inspector General of the Israel Police or the Head of the Intelligence Division. In practice, requests are sent to the Directorate of Courts and then forwarded by them to the Legal Assistance Unit of the Israel Police who oversees the execution of the requests by the competent authorities. In certain cases,the Legal Assistance Unit will consult with the Department of International Affairs regarding the execution of a request.

Procedure		
International Best Practice	**National Legislation**	**Comments**
		While decisions regarding the execution of requests may be made by the Department for International Affairs of the State Attorney's Office and by the Legal Assistance Unit, only the Minister of Justice is authorized to deny an incoming request. A request for legal assistance shall specify the type of proceeding for which the assistance is requested, the facts that constitute the foundation for the suspicion of the commission of an offence, and the connection to the assistance requested. In a request for assistance of this kind, consideration shall be had, inter alia, for whether it complies with the requirements of Israeli law for issuing a warrant for wiretapping, as stipulated above The Police execute the measures requested within the framework of the request.
Article 20 BC - **Real-time collection of traffic data** 1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a. collect or record through the application of technical means on the territory of that Party, and b. compel a service provider, within its existing technical capability: i. to collect or record through the application of technical means on the territory of that Party; or ii. to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.	**Criminal Procedure (Enforcement Powers - Communications Data) 5768 - 2007** **Article 3(g)** **Communications Law (1982)** **Article 13(b)(2)**	**Legal Analysis** Article 3(g) of the Criminal Procedure (Enforcement Powers - Communications Data) 5768 - 2007 and Article 13(b)(2) of the Israeli Communications Law (1982) allow for the collection of traffic data real-time.

Procedure		
International Best Practice	**National Legislation**	**Comments**
2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory. 3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.		
Disclosure obligation of encryption keys		**Legal Analysis** With terrorists and organized criminals routinely using encrypted messaging applications[199] this may be considered a viable power to release the keys to passwords to unlock devices[200] **Gap Analysis** **Recommendation:** There are no decryption powers in Israel – such a provision is recommended to allow law enforcement to compel owners to provide pin codes and passwords to unlock devices
Data retention obligations[201]		**Legal Analysis** Such a power can allow law enforcement to 1. Trace and identify the source of a communication 2. Identify the destination of a communication; 3. Identify the date, time and duration of a communication; and 4. Identify the type of communication

[199] Eleanor Saitta. "Can Encryption Save Us?" Nation 300, no. 24 (June 15, 2015): 16-18. Academic Search Premier, EBSCOhost (accessed February 29, 2016).

[200] For an example see section 49 Regulation of Investigatory Powers Act 2000 (UK) - http://www.legislation.gov.uk/ukpga/2000/23/section/49

[201] See above re 2006 EU Data Retention Directive and EU member state schemes see: http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention

Procedure

International Best Practice	National Legislation	Comments
		The Israeli data protection and privacy laws do not include specific limitations regarding the period for which records must be retained. However, specific requirements do exist with regard to certain kinds of data, such as medical (especially in hospitals) and credit data, which dictate that the relevant data be retained for specific minimum periods. Also, as part of draft guidelines published by the Israeli Law, Information and Technology Authority (ILITA) with regard to identification numbers, ILITA has interpreted the term 'consent' of an individual as meaning an individual's consent to the records being retained as long as required (and no longer). No explicit restriction has been imposed on the period for which an organisation may (or must) retain records.

International Cooperation

International Best Practice	National Legislation	Comments
Article 22 BC - **Jurisdiction** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: a. in its territory; or b. on board a ship flying the flag of that Party; or c. on board an aircraft registered under the laws of that Party; or d. by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.	**Penal Law 1977** **Article 7(a)(1)** **Article 7(c)** **Article 15(a)**	**Legal Analysis** National legislation ensures jurisdiction is defined using the language of Article 22 BC (subject to Israel's reservation of paragraph 1.d.) If there is a conflict between jurisdictions consideration should be given to guidelines on determining the appropriate jurisdiction to try an offence – see the Eurojust Guidelines for Deciding which Jurisdiction should Prosecute (revised 2016)[202]

[202] http://www.eurojust.europa.eu/Practitioners/operational/Documents/Operational-Guidelines-for-Deciding.pdf

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
2. Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 3. Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition. 4. This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. 5. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.		
Article 35 BC **24/7 Network** 1. Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:	**In place**	**Legal Analysis** This is an essential mechanism for an effective international cybercrime investigative capability and is a mandatory requirement of ratification of the BC The National Cyber Center at Lahav 433 (NCC) operates as required by the BC as part of the 24/7 Network

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
a. the provision of technical advice; b. the preservation of data pursuant to Articles 29 and 30; c. the collection of evidence, the provision of legal information, and locating of suspects. 2. a. A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis. b. If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to coordinate with such authority or authorities on an expedited basis. 3. Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.		
Article 25 BC - **General principles relating to mutual assistance** 1. The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. 2. Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.	**International Legal Assistance Law 5758-1998** **Sections 2-11** **Section 5(a)(4)** **Section 8(b)**	**Legal Analysis** Article 25 BC ensures that it can be used as an instrument to facilitate MLA for Israel. The International Legal Assistance Law 5758-1998 Section 8(b) provides that any foreign State's request for legal assistance shall be executed only if the act is permissible under Israeli Law. According to section 5(a)(4) of the International Legal Assistance Law 5758-1998 the Israeli Minister of Justice may refuse a mutual legal assistance request if the request is based on a fiscal offence. However, the offences in sections 2 through 11 to the convention are excluded from the term "fiscal offence", as it is defined in section 1 of the International Legal Assistance Law 5758-1998

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
3. Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party.The requested Party shall accept and respond to the request by any such expedited means of communication. 4. Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation.The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence. 5. Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.		Consideration should be given to allowing adjudicating authorities to authorise domestic law enforcement to investigate in the State where access to a device is known. Accessibility of information is the essential criterion to initiate an investigation in cases where it is not possible to know where the data is stored (i.e. in the cloud). This could include a "mutual recognition" of court orders issued towards communication service providers in a given State, that could be served to branches of that CSPs located in other States, depending on where the data is stored.

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
Article 26 BC - **Spontaneous Information** 1. A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter. 2. Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information	**No equivalent**	**Legal Analysis** This is an important procedure to enable a State privy to information that will assist another state to prevent a cybercrime or to investigate it. Israel can share such information if appropriate.
Article 32 BC – Trans-Border A Party may, without the authorisation of another Party: a. access publicly available (open source) stored computer data, regardless of where the data is located geographically; or b. access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.	**No equivalent**	**Legal Analysis** This procedural power enables a State to secure content stored in another state in limited circumstances. Article 32.b. BC is an exception to the principle of territoriality and permits unilateral trans-border access without the need for mutual legal assistance where there is consent or the information is publicly available. Examples of use of this procedural power under BC Article 32.b. include: A person's e-mail may be stored in another country by a service provider, or a person may intentionally store data in another country. These persons may retrieve the data and, provided that they have the lawful authority, they may voluntarily disclose the data to law enforcement officials or permit such officials to access the data[203]

[203] Paragraph 294, page 53BC Explanatory Report

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
		A suspected terrorist is lawfully arrested while his/her mailbox – possibly with evidence of a crime – is open on his/her tablet, smartphone or other device. If the suspect voluntarily consents that the police access the account and if the police are sure that the data of the mailbox is located in another state, police may access the data under Article 32.b. If information is open source (such as Facebook) there is no prohibition concerning, collection - any person is authorized to access those pages, including a police officer. Israeli Police also routinely request consent to secure computer data stored in another jurisdiction.

Jordan

Jordan has ratified CITO and recently enacted the Cybercrime Law No. 27 of 2015.

Offences		
International Best Practice	**National Legislation**	**Comments**
Article 2 BC **Illegal access** Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.	**Cybercrime Law No.27 of 2015** **Article 3** 1. Anyone who intentionally accesses an information network in any manner without authorization or in violation or excess of an authorization.	**Legal Analysis** Reference is made to illegal access to an *"information network"* which is defined in Article 2 as, « correlation between more than information system to allow data and information and access system. » An « Information system » is defined in Article 2 as « programs and tools developed for the establishment of a set of data or information electronically, or sent, received or processed or stored or managed or displayed by electronic means. » The Article 12(a) offence is an aggravated form for illegal access to computers related to critical infrastructure.

Offences		
International Best Practice	**National Legislation**	**Comments**
	Article 12(a) a. Whoever entered intentionally without a permit or in violation of, or exceeding authorization to the Internet or an information system by any means in order to obtain the data or information not available to the public and affects national security or foreign relations of the Kingdom, public safety or the national economy	**Gap Analysis** **Recommendation:** The translation of the legislation is not clear - but the definition of an information network appears to be similar to that of a computer system[204] in the BC as it implies processing of data. If so, this Article is consistent with international norms.
Article 3 BC **Illegal Interception**	**Cybercrime Law No.27 of 2015** **Article 5** Anyone who intentionally captures, interferes or intercepts what is transmitted through an information network or any information system	**Legal Analysis** This offence is essential to prosecute transmissions of computer data to, from, or within a computer system that may be illegally intercepted to obtain information (e.g. wikileaks or Panama Papers). The offence as drafted is consistent with international best practice
Article 4 BC **Data Interference** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.	**Cybercrime Law No.27 of 2015** **Article 3(b) and (c)** (b) Where the access stipulated in paragraph (a) of this Article is for the purpose of canceling, deleting, adding, destroying, disclosing, destruction of, obscure, amend, modify, move, copy or disable the operation of an information network (c) Whoever entered intentionally to a website to change or cancel or destroy or modify its contents or his occupation or impersonate described or impersonate the owner	**Legal Analysis** Article 3(b) refers to the Article 3(a) offence and access to an information network without authorization with intent to interfere with data. Articles 3(c) in relation to a website does not refer to data interference "without authorization" BC refers to "without right" in Article 4 on the basis the access is unauthorized. The BC Explanatory Report confirmed the derivation of "*without right*" as, "*conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law.*"[205]

[204] See Article 1.a. BC: "*any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data*" **or** section 3(5) HIPCAR: "*a device or a group of inter-connected or related devices, including the Internet, one or more of which, pursuant to a program, performs automatic processing of data or any other function.*"

[205] Paragraph 38, page 8 Explanatory Report to the Convention on Cybercrime – No.185 https://rm.coe.int/16800cce5b

Offences		
International Best Practice	**National Legislation**	**Comments**
	Article 12(c) If the entry referred to in paragraph (a) of this Article was with intent to cancel such data or information, damage, destroy or alter, change or move or copy or disclose	The national legislation does not include suppression of computer data which is an element of phishing often used to secure illegal access by installing a keylogger to obtain sensitive information.[206] Article 12(c) relates to an aggravated offence of data interference impacting critical infrastructure (paragraph 12 (a) refers to without authorization). **Gap Analysis** **Recommendation:** The national legislation should add the act of "*suppression*" "*Without authorization*" should be included in Article 3(c) so consistent with Article 3(b). At present the law is drafted as a strict liability offence, so an accused could be convicted of any modification of website. The Judicial Police would be protected by Article 13(b) – but others who may assist with investigations or those who legitimately change data in websites would not be protected.
Article 5 BC **System Interference**	**Cybercrime Law No.27 of 2015** **Article 4** Who ever enters or uses intentionally programs via the Internet or by using an information system in order to cancel or delete, add, or destruction, disclosure or destruction of, obscure, or amend, modify or transfer, copy, capture, or to enable others to see the data or Information inhibition or interference or shut down or disrupt the work of an information system or access or change the website or canceled or destroy or modify its contents or impersonate the owner without authorization or in excess of authority	**Legal Analysis** Article 4 provides for a system interference offence. Whilst data interference and illegal access have an aggravated offence for impacting critical infrastructure there is no equivalent for system interference. **Gap Analysis** **Recommendations:** Another offence should be considered of prevention and prosecution of attacks against critical infrastructure that hinder the functioning of a computer system – for example hindering the system that stores stock exchange records can make them inaccurate.[207] Reference is made to "*websites*" or "*information system*" consider reference to "*computer systems*" or "*computer networks*" and "*data*" – this will be consistent with BC and CITO. The national legislation should include references to "*computer systems*", "*computer networks*" and "*data*"

[206] http://www.coe.int/en/web/cybercrime/guidance-notes

[207] http://www.coe.int/en/web/cybercrime/guidance-notes

Offences		
International Best Practice	**National Legislation**	**Comments**
Article 6 BC **Misuse of Devices** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a. the production, sale, procurement for use, import, distribution or otherwise making available of: i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5; ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b. the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.	**No equivalent**	**Legal Analysis** This offence will enable prosecution for the production, sale, procurement for use, import, distribution of access codes and other computerized data used to commit cybercrimes. These are elements often present in malware prosecutions. Any offence would also have to consider those devices that have a legitimate as well as being put to criminal use (“*dual use*”) – this should include the BC language of *“primarily adapted”* **Gap Analysis** **Recommendation:** The national legislation should include an offence using relevant language from BC, CITO or HIPCAR to ensure any access is without authorization and any devices *“primarily”* adapted to commit the offence Please note that HIPCAR provides the option of listing the devices in a schedule if deemed appropriate – this could be restrictive and require updating with technological progress. The national law should provide a reasonable excuse so law enforcement can use devices for special investigation techniques – the language at Article 6.2. BC or section 10(2) HIPCAR can be used as a guide.

Offences		
International Best Practice	**National Legislation**	**Comments**
2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3. 3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article **Section 10 HIPCAR – Illegal Devices** 1. A person commits an offence if the person: a. intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, produces, sells, procures for use, imports, exports, distributes or otherwise makes available: i. a device, including a computer program, that is designed or adapted for the purpose of committing an offence defined by other provisions of Part II of this law; or ii. a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed;		

Offences		
International Best Practice	National Legislation	Comments
with the intent that it be used by any person for the purpose of committing an offence defined by other provisions of Part II of this law; or b. has an item mentioned in subparagraph (i) or (ii) in his or her possession with the intent that it be used by any person for the purpose of committing an offence defined by other provisions of part II of this law commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. 2. This provision shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 is not for the purpose of committing an offence established in accordance with other provisions of Part II of this law, such as for the authorized testing or protection of a computer system. 3. A country may decide not to criminalize illegal devices or limit the criminalization to devices listed in a Schedule.		

Offences		
International Best Practice	National Legislation	Comments
Article 7 BC **Computer Related Forgery** Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches. **Article 10 CITO** **Offence of Forgery** The use of information technology means to alter the truth of data in a manner that causes harm, with the intent of using them as true data. **Section 11 HIPCAR – Computer-related Forgery** 1. A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification inputs, alters, deletes, or suppresses computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.	**Cybercrime Law No.27 of 2015** **Article 4** Who ever enters or uses intentionally programs via the Internet or by using an information system in order to cancel or delete, add, or destruction, disclosure or destruction of, obscure, or amend, modify or transfer, copy, capture, or to enable others to see the data or Information inhibition or interference or shut down or disrupt the work of an information system or access or change the website or canceled or destroy or modify its contents or impersonate the owner without authorization or in excess of authority	**Legal Analysis** This offence only refers to impersonating the owner and includes no reference to dishonest intent and is more relevant to a system interference offence. Incorporation of BC article 7 or section 11 HIPCAR is advised to protect against this offending which could include phishing and spear phishing For example, computer data (such as the data used in electronic passports) may be input, altered, deleted, or suppressed with the result that inauthentic data is considered or acted upon for legal purposes as if it were authentic.[208] Section 11(2) HIPCAR also provides for the sending of multiple electronic email messages as an aggravated offence. The language in Article 10 CITO has no reference to any dishonest intent and requires harm to be caused – the language in BC and HIPCAR is to be preferred as it does not require harm to be caused. BC and HIPCAR only requires that the "*inauthentic data*" data is "*considered*" **Gap Analysis** **Recommendation:** Use the BC language in Article 7, or section 11 HIPCAR as a guide for national legislation

[208] http://www.coe.int/en/web/cybercrime/guidance-notes

Offences		
International Best Practice	**National Legislation**	**Comments**
2. If the abovementioned offence is committed by sending out multiple electronic mail messages from or through computer systems, the penalty shall be imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.		
Article 8 BC **Computer related fraud** Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a. any input, alteration, deletion or suppression of computer data, b. any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person. **Section 12 HIPCAR – Computer-related Fraud** A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification causes a loss of property to another person by: c. any input, alteration, deletion or suppression of computer data; d. any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person the penalty shall be imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.	**Cybercrime Law No.27 of 2015** **Article 6** Anyone who intentionally and without authorization obtains through an information network or any information system data or information relating to credit cards or data or information that is used in execution of electronic financial or banking transactions **Article 7** Whoever commits one of the acts stipulated in Articles 3, 4, 5 or 6 of this law in relation to an information system or website or the information network concerning the transfer of the money, or providing payment services or clearing or settlement or any of the banking services provided by banks and financial companies	**Legal Analysis** This offence only relates to the obtaining and using of credit card or financial banking transaction data without authorization. It would not cover all types of phishing or other types of cyber fraud, such as identity theft. A fraud would require a false misrepresentation or dishonest intent – it does not rely upon the data being either obtained or used. A computer fraud relates to a perpetrator intending to gain an economic benefit for himself or another. It isn't always necessary to prove or demonstrate that loss. **Gap Analysis** **Recommendation:** A fraud offence with dishonest intent is included to encapsulate all types of computer-related fraudulent activity – use section 12 of HIPCAR or Article 8 BC

Offences		
International Best Practice	**National Legislation**	**Comments**
Article 9 **Content related offences (e.g. child pornography)** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a. producing child pornography for the purpose of its distribution through a computer system; b. offering or making available child pornography through a computer system; c. distributing or transmitting child pornography through a computer system; d. procuring child pornography through a computer system for oneself or for another person; e. possessing child pornography in a computer system or on a computer-data storage medium. 2. For the purpose of paragraph 1 above, the term “child pornography” shall include pornographic material that visually depicts: a. a minor engaged in sexually explicit conduct; b. a person appearing to be a minor engaged in sexually explicit conduct; c. realistic images representing a minor engaged in sexually explicit conduct. 3. For the purpose of paragraph 2 above, the term “minor” shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.	**Cybercrime Law No.27 of 2015** **Article 9** a. Any person who intentionally sends or disseminates audible or visual information, through information systems or information networks, which includes anything related to pornography or sexual exploitation for those who did not complete the age of eighteen will be punished. b. Any person who intentionally uses an information system or information network to create, prepare, save, display, print, or publish or promote activities or acts of pornography for the purpose of influencing those who are not eighteen years of age, or the psychologically or mentally disabled, or directing and inciting them to commit a crime. c. Whoever has deliberately used an information system or information network for the purposes of exploitation of those who have not completed eighteen years of age or who are disabled psychologically or mentally, in prostitution or pornography	**Legal Analysis** This is an essential offence in order to protect children from harm by criminalizing the distribution, transmitting, making available, offering, producing and possession of indecent images of children. The national legislation has a focus on distributing or using an “*information system or information network*” to create the pornography. This offence does not include possession or offer or making available or procuring for another person. There are no definitions of “*pornography*”, “*create*”, “*prepare*”, “*save*”, “*display*”, “*print*”, “*publish*”, or “*promote activities or acts of pornography*” Paragraph c. specifically relates to child sexual exploitation – but is not specific to the production, or possession of indecent images of children **Gap Analysis** **Recommendation:** The language in BC Article 9 or section 13 HIPCAR is preferred to protect children and prosecute perpetrators

Offences		
International Best Practice	**National Legislation**	**Comments**
4. Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c. **Section 13 HIPCAR – Child Pornography** 1. A person who, intentionally, without lawful excuse or justification: • produces child pornography for the purpose of its distribution through a computer system; • offers or makes available child pornography through a computer system; • distributes or transmits child pornography through a computer system; • procures and/or obtain child pornography through a computer system for oneself or for another person; • Possesses child pornography in a computer system or on a computer- data storage medium; or • knowingly obtains access, through information and communication technologies, to child pornography, commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. 2. It is a defense to a charge of an offence under paragraph (1) (b) to (1)(f) if the person establishes that the child pornography was a bona fide law enforcement purpose. 3. A country may not criminalize the conduct described in section 13 (1) (d)- (f).		

Offences

International Best Practice	National Legislation	Comments
Article 10 BC **Infringement of Copyright** **Article 17 CITO - Offenses Related to Copyright and Adjacent Rights**	1. Books, brochures and other written materials. 2. Works that have the brink of lectures, speeches and preaching. 3. Theatrical works and musical and musical plays and theatrical representation. 4. Musical works, whether numbered or not, or accompanied by words or not. 5. Cinematic and audiovisual works. 6. Painting, painting, sculpture, engraving, architecture, applied and decorative arts. 7. Illustrations, maps, designs, sketches and stereotypes relating to geography and surface maps of the land. 8. Software programs whether in the source language or machine language C. Protection shall include the title of the work only if the title is an ongoing term to denote the subject of the work.	**Legal Analysis** This provision ensures protection of innovation in the 21st century of the SPCs, businesses and citizens. Additionally, it protects the collection of literary or artistic works such as encyclopedias, anthologies and collected data, either in machine-readable form or in any other form, and in terms of the selection or arrangement of their contents they constitute creative works of art. The collections containing selected extracts of poetry, prose or music Or others to mention in those collections the source of the extracts and their authors without prejudice to the rights of the authors in respect of each work forming part of these collections
Article 11 BC **Aiding and Abetting** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.	**Cybercrime Law No.27 of 2015** **Article 14** Any person who intentionally or jointly intervene or incitement to commit any of the crimes stipulated in this Law, the penalty specified therein for the perpetrators punished applies	**Legal Analysis** Aiding and abetting others to commit offences is essential in order to prosecute those who may have provided assistance or encouraged cybercrimes to take place. Article 19 CITO also includes attempt which is not included in Article 14 **Gap Analysis** **Recommendation:** Incorporate Article 19 CITO (where no reference to attempt in Jordan) as a guide for national legislation

Offences		
International Best Practice	**National Legislation**	**Comments**
2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention. **Article 19 CITO - Attempt at and Participation in the Commission of Offences** 1. Participation in the commission of any of the offences set forth in this chapter with the intention to commit the offence in the law of the State Party. 2. Attempt at the commission the offences set forth in Chapter II of this convention. 3. A State Party may reserve the right to not implement the second paragraph of this Article totally or partly.		
Article 12 BC[209] **Corporate liability**	**Code of Criminal Procedure**	**Legal Analysis** This provision is an essential element so that legal persons (e.g. corporate entities) acting on behalf of natural persons have criminal liability
Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems **Article 3 – Dissemination of racist and xenophobic material through computer systems** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:	**Penal Code**	**Gap Analysis** **Recommendation:** Use the BC language in Article 3 Additional Protocol as a guide for national legislation where any gaps are identified

[209] Article 20 CITO

Offences		
International Best Practice	National Legislation	Comments
distributing, or otherwise making available, racist and xenophobic material to the public through a computer system. 2. A Party may reserve the right not to attach criminal liability to conduct as defined by paragraph 1 of this article, where the material, as defined in Article 2, paragraph 1, advocates, promotes or incites discrimination that is not associated with hatred or violence, provided that other effective remedies are available. 3. Notwithstanding paragraph 2 of this article, a Party may reserve the right not to apply paragraph 1 to those cases of discrimination for which, due to established principles in its national legal system concerning freedom of expression, it cannot provide for effective remedies as referred to in the said paragraph 2.		
Additional Protocol **Article 4[210] – Racist and xenophobic motivated threat** Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: threatening, through a computer system, with the commission of a serious criminal offence as defined under its domestic law, (i) persons for the reason that they belong to a group, distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors, or (ii) a group of persons which is distinguished by any of these characteristics.	**Article 278** A penalty of imprisonment for a period not exceeding three months or a fine not exceeding twenty dinars shall be punishable by: 1. Publish a printed, manuscript, picture, drawing or symbol that would insult the religious feeling of other people or insult their religious belief; 2. Speak in a public place and on hearing from another person with a word or voice that would insult the religious feeling or belief of that other person	**Legal Analysis** Article 278 is linked to Article 15 of Electronic Crimes Law No. 27 of 2015 which stipulates that any person who commits any crime punishable under any applicable legislation using the information network or any information system or website, or participates in or instigates or instigates the commission thereof shall be punished by the penalty provided for in that legislation **Gap Analysis** **Recommendation:** Article 278 only refers to religious insult and not the wider offence of xenophobic or racist threats. Further, there is no reference to the mens rea of intentionally or without right – or of the conduct being threatening. Use the BC language in Article 4 Additional Protocol as a guide for national legislation

[210] no equivalent in CITO

Offences		
International Best Practice	**National Legislation**	**Comments**
Additional Protocol **Article 5[211] - Racist and xenophobic motivated insult** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: insulting publicly, through a computer system, (i) persons for the reason that they belong to a group distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors; or (ii) a group of persons which is distinguished by any of these characteristics. 2. A Party may either: a. require that the offence referred to in paragraph 1 of this article has the effect that the person or group of persons referred to in paragraph 1 is exposed to hatred, contempt or ridicule; or b. reserve the right not to apply, in whole or in part, paragraph 1 of this article.	**Penal Code**	**Legal Analysis** The relevant article is linked to Article 15 of Electronic Crimes Law No. 27 of 2015 which stipulates that any person who commits any crime punishable under any applicable legislation using the information network or any information system or website, or participates in or instigates or instigates the commission thereof shall be punished by the penalty provided for in that legislation **Gap Analysis** **Recommendation:** Use the BC language in Article 5 Additional Protocol as a guide for national legislation where any gaps are identified

[211] no equivalent in CITO

Offences		
International Best Practice	**National Legislation**	**Comments**
Additional Protocol **Article 6[212] - Denial, gross minimisation, approval or justification of genocide or crimes against humanity** 1. Each Party shall adopt such legislative measures as may be necessary to establish the following conduct as criminal offences under its domestic law, when committed intentionally and without right: distributing or otherwise making available, through a computer system to the public, material which denies, grossly minimises, approves or justifies acts constituting genocide or crimes against humanity, as defined by international law and recognised as such by final and binding decisions of the International Military Tribunal, established by the London Agreement of 8 August 1945, or of any other international court established by relevant international instruments and whose jurisdiction is recognised by that Party. 2. A Party may either a. require that the denial or the gross minimisation referred to in paragraph 1 of this article is committed with the intent to incite hatred, discrimination or violence against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors, or otherwise b. reserve the right not to apply, in whole or in part, paragraph 1 of this article.	**Penal Code**	**Legal Analysis** The relevant article is linked to Article 15 of the Electronic Crimes Law No. 27 of 2015 which stipulates that any person who commits any crime punishable under any applicable legislation using the information network or any information system or website, or participates in or instigates or instigates the commission thereof shall be punished by the penalty provided for in that legislation **Gap Analysis** **Recommendation:** Use the BC language in Article 6 Additional Protocol as a guide for national legislation where any gaps are identified

[212] no equivalent in CITO

Offences		
International Best Practice	**National Legislation**	**Comments**
Additional Offences to Review		
Identity-related Crimes **Section 14 HIPCAR** A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification by using a computer system in any stage of the offence, intentionally transfers, possesses, or uses, without lawful excuse or justification, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a crime, commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.	**Electronic Crimes Law** **No. 27 of 2015** **Article 15** Any person who commits any crime punishable under any applicable legislation using the information network or any information system or website or participates in or interferes or incites to commit them shall be punished by the penalty provided for in that legislation.	**Legal Analysis** Whilst Article 15 criminalises any substantive offence that uses an information network, information system or website – no offence has been identified in Jordanian that covers the preparation phase of an identity–related crime of dishonesty. **Gap Analysis** **Recommendation:** Inclusion in domestic legislation is advisable.
Disclosure of Details of an Investigation **Section 16 HIPCAR** An Internet service provider who receives an order related to a criminal investigation that explicitly stipulates that confidentiality is to be maintained or such obligation is stated by law and intentionally without lawful excuse or justification or in excess of a lawful excuse or justification discloses: • the fact that an order has been made; or • anything done under the order; or • any data collected or recorded under the order; commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.		**Legal Analysis** This offence sanctions data breaches and disclosure of sensitive information that could impact criminal investigations **Gap Analysis** **Recommendation:** Inclusion in domestic legislation is advisable.

Offences		
International Best Practice	**National Legislation**	**Comments**
Failing to Permit Assistance **Section 17 HIPCAR** 1. A person other than the suspect who intentionally fails without lawful excuse or justification or in excess of a lawful excuse or justification to permit or assist a person based on an order as specified by sections 20 to 22[213] commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. 2. A country may decide not to criminalize the failure to permit assistance provided that other effective remedies are available.		**Legal Analysis** This offence relates to persons, with specific knowledge of relevant evidence, who refuse to assist. Often law enforcement will be reliant upon such persons to secure evidence in cyber investigations. A separate offence is the failure to provide passwords or access to codes to encrypted devices or data (i.e. *"key to protected information")* – section 53 of the UK Regulation of Investigatory Powers Act 2000 (RIPA) [214] provides for a criminal offence for persons who fail to comply with a section 49 RIPA Notice to disclose the *"key"* **Gap Analysis** **Recommendation:** Inclusion in domestic legislation is advisable.
Cyber Stalking **Section 18 HIPCAR** A person, who without lawful excuse or justification or in excess of a lawful excuse or justification initiates any electronic communication, with the intent to coerce, intimidate, harass, or cause substantial emotional distress to a person, using a computer system to support severe, repeated, and hostile behavior, commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.		**Legal Analysis** This offence criminalizes those who harass persons online– some jurisdictions may have non-computer related harassment offences – but this offence is recommended for those crimes committed online. **Gap Analysis** **Recommendation:** Inclusion in domestic legislation is advisable.

[213] Search and seizure, assistance and production orders

[214] http://www.legislation.gov.uk/ukpga/2000/23/section/53

Offences		
International Best Practice	**National Legislation**	**Comments**
Grooming Children Online **Dutch Criminal Code 248e** The person who proposes to arrange a meeting, by means of an automated work or by making use of a communication service, to a person of whom he knows, or should reasonably assume, that such person has not yet reached the age of sixteen, with the intention of committing indecent acts with this person or of creating an image of a sexual act in which this person is involved, will be punished with a term of imprisonment of at most two years or a fine of the fourth category, if he undertakes any action intended to realise that meeting. **Canadian Criminal Code** **Section 172.1** 1. Every person commits an offence who, by a means of telecommunication, communicates with a. a person who is, or who the accused believes is, under the age of 18 years, for the purpose of facilitating the commission of an offence under subsection 153(1), section 155, 163.1, 170 or 171 or subsection 212(1), (2), (2.1) or (4) with respect to that person; b. a person who is, or who the accused believes is, under the age of 16 years, for the purpose of facilitating the commission of an offence under section 151 or 152, subsection 160(3) or 173(2) or section 271, 272, 273 or 280 with respect to that person; or		**Legal Analysis** To prove the Dutch offence a meeting for sexual purposes is required with supporting evidence of online chat history with sexual intent; request for a meeting with evidence this was planned (i.e. date and place). The purpose of the Canadian law is to prevent grooming by predatory adults of children online. This offence does not require the sexual offence to have occurred. This means the accused does not need to have actually gone to meet the victim in person. The offence is committed before any actions are taken to commit the substantive offence. **Gap Analysis** **Recommendation:** Inclusion in domestic legislation is advisable to criminalise this preparatory behaviour before a sexual offence is committed

Offences		
International Best Practice	**National Legislation**	**Comments**
c. a person who is, or who the accused believes is, under the age of 14 years, for the purpose of facilitating the commission of an offence under section 281 with respect to that person. Punishment 2. Every person who commits an offence under subsection (1) is guilty of a. is guilty of an indictable offence and is liable to imprisonment for a term of not more than 10 years and to a minimum punishment of imprisonment for a term of one year; or b. is guilty of an offence punishable on summary conviction and is liable to imprisonment for a term of not more than 18 months and to a minimum punishment of imprisonment for a term of 90 days. Presumption re age 3. Evidence that the person referred to in paragraph (1)(a), (b) or (c) was represented to the accused as being under the age of eighteen years, sixteen years or fourteen years, as the case may be, is, in the absence of evidence to the contrary, proof that the accused believed that the person was under that age. No defence 4. It is not a defence to a charge under paragraph (1)(a), (b) or (c) that the accused believed that the person referred to in that paragraph was at least eighteen years of age, sixteen years or fourteen years of age, as the case may be, unless the accused took reasonable steps to ascertain the age of the person.		

Procedure		
International Best Practice	**National Legislation**	**Comments**
Article 19 BC[215] **Search and seizure of stored computer data** 1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a. a computer system or part of it and computer data stored therein; and b. a computer-data storage medium in which computer data may be stored in its territory. 2. Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a. seize or similarly secure a computer system or part of it or a computer-data storage medium;	**Cybercrime Law No.27 of 2015** **Article 13** A. Taking into account the terms and conditions prescribed in the legislation in force and taking into account the personal rights of the defendant, Judicial Police employees may, after obtaining permission from the Attorney General concerned or of the competent court, access anywhere with indications of being used to commit any of the offences set forth in this law, also they may inspect the equipment, tools, programs, regulations and the means by which the evidence suggest that they are used to commit any of those crimes, and in all cases, the employee who inspected shall draw up the minutes of this and submit it to the competent prosecutor.	**Legal Analysis** This the most essential investigatory power and should refer to gaining access than search. In the BC Explanatory Report, *"Search"* means to seek, read, inspect or review data. It includes the notion of searching for data and searching of (examining) data. The word *"access"* has a neutral meaning and reflects more accurately computer terminology – further this is used in Articles 26 and 27 CITO.[216] **Gap Analysis** **Recommendation:** There should be a specific reference to *seizure* as set out in Article 27 CITO. A definition of "*seize*" to insure integrity and to specific procedures is advisable – see section 3(16) HIPCAR "*Seize includes:* • *activating any onsite computer system and computer data storage media;* • *making and retaining a copy of computer data, including by using onsite equipment;* • *maintaining the integrity of the relevant stored computer data;* • *rendering inaccessible, or removing, computer data in the accessed computer system;* • *taking a printout of output of computer data; or* • *seize or similarly secure a computer system or part of it or a computer- data storage medium.*" Section 21 HIPCAR provides for legislation to ensure assistance is provided by those who have specialist knowledge of the location of relevant evidence – this could be used as a guide – also see section 17 HIPCAR for an offence if assistance is refused without lawful excuse

[215] Articles 26 and 27 CITO

[216] Paragraph 191, page 33 Explanatory Report BC

Procedure		
International Best Practice	National Legislation	Comments
b. make and retain a copy of those computer data; c. maintain the integrity of the relevant stored computer data; d. render inaccessible or remove those computer data in the accessed computer system. 4. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2. 5. The powers and procedures referred to in this article shall be subject to Articles 14 and 15. **Section 20 HIPCAR – Search and Seizure** 1. If a [judge] [magistrate] is satisfied on the basis of [information on oath] [affidavit] that there are reasonable grounds [to suspect] [to believe] that there may be in a place a thing or computer data: • that may be material as evidence in proving an offence; or • that has been acquired by a person as a result of an offence; the [judge] [magistrate] [may] [shall] issue a warrant authorizing a [law enforcement] [police] officer, with such assistance as may be necessary, to enter the place to search and seize the thing or computer data including search or similarly access:		

Procedure		
International Best Practice	**National Legislation**	**Comments**
i. a computer system or part of it and computer data stored therein; and ii. a computer-data storage medium in which computer data may be stored in the territory of the country. 2. If [law enforcement] [police] officer that is undertaking a search based on Sec. 20 (1) has grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, he shall be able to expeditiously extend the search or similar accessing to the other system. 3. A [law enforcement] [police] officer that is undertaking a search are empowered to seize or similarly secure computer data accessed according to paragraphs 1 or 2. **Section 21 HIPCAR – Assistance** Any person who is not a suspect of a crime but who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein that is the subject of a search under section 20 must permit, and assist if reasonably required and requested by the person authorized to make the search by: • providing information that enables the undertaking of measures referred to in section 20; • accessing and using a computer system or computer data storage medium to search any computer data available to or in the system; • obtaining and copying such computer data;		

Procedure		
International Best Practice	**National Legislation**	**Comments**
• using equipment to make copies; and • obtaining an intelligible output from a computer system in such a format that is admissible for the purpose of legal proceedings. **Article 26 CITO - Inspecting Stored Information** 1. Every State Party shall commit itself to adopting the procedures necessary to enable its competent authorities to inspect or access: a. an information technology or part thereof and the information stored therein or thereon. b. the storage environment or medium in or on which the information may be stored. 2. Every State Party shall commit itself to adopting the procedures necessary to enable the competent authorities to inspect or access a specific information technology or part thereof in conformity with paragraph 1(a) if it is believed that the required information is stored in another information technology or in part thereof in its territory and such information is legally accessible or available in the first technology, the scope of inspection may be extended and the other technology accessed.		

Procedure		
International Best Practice	**National Legislation**	**Comments**
Article 27 CITO - Seizure of Stored Information 1. Every State Party shall commit itself to adopting the procedures necessary to enable the competent authorities to seize and safeguard information technology information accessed according to Article 26, paragraph 1, of this Convention. These procedures include the authority to: a. seize and safeguard the information technology or part thereof or the storage medium for the information technology information. b. make a copy the information technology information and keep it. c. maintain the integrity of the stored information technology information. d. remove such accessed information from the information technology or prevent its access. 2. Every State Party shall commit itself to adopting the procedures necessary to enable the competent authorities to order any person who is acquainted with the functioning of the information technology or the procedures applied to protect the information technology to give the information necessary to complete the procedures mentioned in paragraphs 2 and 3 of Article 26 of this Convention.		

Procedure		
International Best Practice	**National Legislation**	**Comments**
Article 16 BC **Expedited preservation of stored computer data** 1. Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2. Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.	**No equivalent**	**Legal Analysis** This procedural power is important to ensure that data which is vulnerable to deletion or loss is preserved. **Gap Analysis** **Recommendation:** This expedited power to retain BSI, metadata, transactional and stored content is essential as part of cybercrime investigations to ensure the evidence is available for search, access, seizure and review. The language of Article 16 of the BC, section 23 HIPCAR or Article 23 CITO could be used. This will also require definitions of *"computer data"*,[217] *"subscriber information or BSI"*, *"traffic data"*[218] and *"Communication Service Provider"*[219] To note BC and HIPCAR do not provide a definition of BSI – but CITO does for subscriber information:[220] *"Any information that the service provider has concerning the subscribers to the service, except for information through which the following can be known:* a. *The type of communication service used, the technical requirements and the period of service.* b. *The identity of the subscriber, his postal or geographic address or phone number and the payment information available by virtue of the service agreement or arrangement* c. *Any other information on the installation site of the communication equipment by virtue of the service agreement."* Consideration should be given the length of preservation that is reasonable in the circumstances and allowing for an application to extend in exigent circumstances – BC and CITO have 90 days and HIPCAR 7 days. From experience 90 days is too few in a cyber investigation and the figure should be nearer 180 days and then subject to extension.

[217] See Article 1.b. BC **or** section 3(6) HIPCAR

[218] See Article 1.d BC: "*any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service*" **or** section 3(18) HIPCAR: "*Traffic data means computer data that: a. relates to a communication by means of a computer system; and b. is generated by a computer system that is part of the chain of communication ; and c. shows the communication's origin, destination, route, time date, size, duration or the type of underlying services.*"

[219] See Article 1.c.BC: "*i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii any other entity that processes or stores computer data on behalf of such communication service or users of such service.*"

[220] See Article 2(9) CITO

Procedure		
International Best Practice	National Legislation	Comments
3. Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. 4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15. **Section 23 HIPCAR – Expedited Preservation** If a [law enforcement] [police] officer is satisfied that there are grounds to believe that computer data that is reasonably required for the purposes of a criminal investigation is particularly vulnerable to loss or modification, the [law enforcement] [police] officer may, by written notice given to a person in control of the computer data, require the person to ensure that the data specified in the notice be preserved for a period of up to seven (7) days as specified in the notice. The period may be extended beyond seven (7) days if, on an ex parte application, a [judge] [magistrate] authorizes an extension for a further specified period of time. **Article 23 CITO - Expeditious Custody of Data Stored in Information Technology** 1. Every State Party shall adopt the procedures necessary to enable the competent authorities to issue orders or obtain the expeditious custody of information, including information for tracking users, that was stored on an information technology, especially if it is believed that such information could be lost or amended.		

Procedure		
International Best Practice	**National Legislation**	**Comments**
2. Every State Party shall commit itself to adopting the procedures necessary as regards paragraph 1, by means of issuing an order to a person to preserve the information technology information in his possession or under his control, in order to require him to preserve and maintain the integrity of such information for a maximum period of 90 days that may be renewed, in order to allow the competent authorities to search and investigate 3. Every State Party shall commit itself to adopting the procedures necessary to require the person responsible for safeguarding the information technology to maintain the procedures secrecy throughout the legal period stated in the domestic law.		
Article 17 BC **Expedited preservation and partial disclosure of traffic data** 1. Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to: a. ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and	**No equivalent**	**Legal Analysis** This procedural power is especially important to ensure that CSPs provide IP addresses that could locate the perpetrator of a cybercrime. The questionnaire confirms that data can be preserved upon receipt of a LOR **Gap Analysis** **Recommendation:** This expedited power alongside disclosure of traffic data should be included in legislation to enable effective investigations of cybercrime. The language of Article 17 of the BC, sections 23 and 24 HIPCAR or Article 24 CITO could be used. This will also require definitions of *"traffic data" and "Communication Service Provider"*[221]

[221] See definitions above

Procedure		
International Best Practice	National Legislation	Comments
b. ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted. 2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15. **Section 23 HIPCAR – Expedited Preservation** If a [law enforcement] [police] officer is satisfied that there are grounds to believe that computer data that is reasonably required for the purposes of a criminal investigation is particularly vulnerable to loss or modification, the [law enforcement] [police] officer may, by written notice given to a person in control of the computer data, require the person to ensure that the data specified in the notice be preserved for a period of up to seven (7) days as specified in the notice. The period may be extended beyond seven (7) days if, on an ex parte application, a [judge] [magistrate] authorizes an extension for a further specified period of time. **Section 24 HIPCAR – Partial Disclosure of Traffic Data** If a [law enforcement] [police] officer is satisfied that data stored in a computer system is reasonably required for the purposes of a criminal investigation, the [law enforcement] [police] officer may, by written notice given to a person in control of the computer system, require the person to disclose sufficient traffic data about a specified communication to identify:		

Procedure		
International Best Practice	**National Legislation**	**Comments**
a. the Internet service providers; and/or b. the path through which the communication was transmitted. **Article 24 CITO - Expeditious Custody and Partial Disclosure of Users Tracking Information** Every State Party shall commit itself to adopting the procedures necessary as regards users tracking information in order to: 1. ensure expeditious custody of users tracking information, regardless of whether such communication is transmitted by one or more service providers. 2. ensure that a sufficient amount of users tracking information is disclosed to the competent authorities of the State Party or to a person appointed by these authorities to allow the State Party to determine the service providers and the transmission path of the communications.		
Article 18 BC[222] **Production Order** 1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a. a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and	**No equivalent**	**Legal Analysis** This is an essential provision for an effective cybercrime investigation and its absence will impact upon prosecutions and international cooperation.

[222] Article 25 CITO

Procedure		
International Best Practice	**National Legislation**	**Comments**
b. a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. 2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 3. For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a. the type of communication service used, the technical provisions taken thereto and the period of service; b. the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c. any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.		**Gap Analysis** **Recommendation:** This essential power is necessary to ensure CSPs in Jordan provide BSI, traffic data and stored content data. This will also require definitions of *"computer data", "subscriber information or BSI", "traffic data" and "Communication Service Provider".*[223] Article 25 CITO is a model that could be used and uses different definitions including *"information technology",*[224] *"service provider"*[225] and *"data"*[226] – it is still advisable to have definitions for *"subscriber information or BSI", "traffic data"* as they will be different types of evidence that can be produced from CSPs. Further, this power will require individuals and others (such as corporate entities, financial institutions and other organisations) who hold data to produce it to law enforcement authorities. Article 18 BC and section 22 HIPCAR could be a guide with consistent application of definitions

[223] See definitions above

[224] Article 2(1) CITO: "*any material or virtual means or group of interconnected means used to store, sort, arrange, retrieve, process, develop and exchange information according to commands and instructions stored therein. This includes all associated inputs and outputs, by means of wires or wirelessly, in a system or network.*"

[225] Article 2(2) CITO: "*any natural or juridical person, common or private, who provides subscribers with the services needed to communicate through information technology, or who processes or stores information on behalf of the communication service or its users.*"

[226] Article 2(3) CITO: "*all that may be stored, processed, generated and transferred by means of information technology, such as numbers, letters, symbols, etc…*"

Procedure		
International Best Practice	**National Legislation**	**Comments**
Section 22 HIPCAR – Production Order If a [judge] [magistrate] is satisfied on the basis of an application by a [law enforcement] [police] officer that specified computer data, or a printout or other information, is reasonably required for the purpose of a criminal investigation or criminal proceedings, the [judge] [magistrate] may order that: • a person in the territory of [enacting country] in control of a computer system produce from the system specified computer data or a printout or other intelligible output of that data; or • an Internet service provider in [enacting country] to produce information about persons who subscribe to or otherwise use the service. **Article 25 CITO - Order to Submit Information** Every State Party shall commit itself to adopting the procedures necessary to enable the competent authorities to issue orders to: 1. Any person in its territory to submit certain information in his possession which is stored on information technology or a medium for storing information. 2. Any service provider offering his services in the territory of the State Party to submit user's information related to that service which is in the possession of the service provider or under his control.		

Procedure		
International Best Practice	**National Legislation**	**Comments**
Article 21 BC[227] **Interception of content data** 1. Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: a. collect or record through the application of technical means on the territory of that Party, and b. compel a service provider, within its existing technical capability: i. to collect or record through the application of technical means on the territory of that Party, or ii. to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.	**Cybercrime Law No.27 of 2015** **Article 13** A. Taking into account the terms and conditions prescribed in the legislation in force and taking into account the personal rights of the defendant, Judicial Police employees may, after obtaining permission from the Attorney General concerned or of the competent court, access anywhere with indications of being used to commit any of the offences set forth in this law, also they may inspect the equipment, tools, programs, regulations and the means by which the evidence suggest that they are used to commit any of those crimes, and in all cases, the employee who inspected shall draw up the minutes of this and submit it to the competent prosecutor.	**Legal Analysis** This Article allows the Judicial Police to intercept communications with permission from the Attorney General **Gap Analysis** **Recommendations:** Provision should be made to compel CSPs in Jordan to cooperate with real-time collection of content for all crimes; and safeguards should be incorporated to ensure that interception and the collection is legal, necessary, reasonable and proportionate in the circumstances. Consideration should be given to reviewing Article 29 of CITO, Article 21 BC and section 26 HIPCAR and incorporating language in national legislation

[227] Article 29 CITO

Procedure		
International Best Practice	**National Legislation**	**Comments**
3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15. **Section 26 HIPCAR – Interception of Content Data** 1. If a [judge] [magistrate] is satisfied on the basis of [information on oath] [affidavit] that there are reasonable grounds to [suspect] [believe] that the content of electronic communications is reasonably required for the purposes of a criminal investigation, the magistrate [may] [shall]: • order an Internet service provider whose service is available in [enacting country] through application of technical means to collect or record or to permit or assist competent authorities with the collection or recording of content data associated with specified communications transmitted by means of a computer system; or authorize a [law enforcement] [police] officer to collect or record that data through application of technical means. 2. A country may decide not to implement section 26.	C. Subject to paragraph (a) of this Article, taking into account the rights of others bona fide, excluding those licensed under the provisions of the Telecommunications Law, who did not participate in any offence under this Act, Judicial Police employees may control the devices, tools, programs, systems and the means used to commit any of the crimes stipulated or covered by this law and the money earned from them and reserve the information and data relating to commit any of them. C. The competent court may rule to confiscate the equipment and tools, stop or disrupt the work of any information system or website used to commit any of the offences set forth or covered by this law, confiscate the money earned from these crimes, and decide to remove the violation at the expense of the perpetrator.	

Procedure		
International Best Practice	**National Legislation**	**Comments**
Article 29 CITO - Interception of Content Information 1. Every State Party shall commit itself to adopting the legislative procedures necessary as regards a series of offences set forth in the domestic law, in order to enable the competent authorities to: a. gather or register through technical means in the territory of this State Party, or b. b.cooperate with and help the competent authorities to expeditiously gather and register content information of the relevant communications in its territory and which are transmitted by means of the information technology. 2. If, because of the domestic legal system, the State Party is unable to adopt the procedures set forth in paragraph 1(a), it may adopt other procedures in the form necessary to ensure the expeditious gathering and registration of content information corresponding to the relevant communications in its territory using the technical means in that territory. 3. Every State Party shall commit itself to adopting the procedures necessary to require the service provider to maintain the secrecy of any information when exercising the authority set forth in this Article.		

Procedure		
International Best Practice	National Legislation	Comments
Article 20 BC[228] **Real-time collection of traffic data** 1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a. collect or record through the application of technical means on the territory of that Party, and b. compel a service provider, within its existing technical capability: i. to collect or record through the application of technical means on the territory of that Party; or ii. to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.		

[228] Article 28 CITO refers to expeditious collection rather than real-time collection

Procedure		
International Best Practice	**National Legislation**	**Comments**
3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15. **Section 25 HIPCAR - Collection of Traffic Data** 1. If a [judge] [magistrate] is satisfied on the basis of [information on oath][affidavit] that there are reasonable grounds to [suspect] [believe] that traffic data associated with a specified communication is reasonably required for the purposes of a criminal investigation, the [judge] [magistrate] [may] [shall] order a person in control of such data to: • collect or record traffic data associated with a specified communication during a specified period; or • permit and assist a specified [law enforcement] [police] officer to collect or record that data. 2. If a [judge] [magistrate] is satisfied on the basis of [information on oath] [affidavit] that there are reasonable grounds to [suspect] [believe] that traffic data is reasonably required for the purposes of a criminal investigation, the [judge] [magistrate] [may] [shall] authorize a [law enforcement] [police] officer to collect or record traffic data associated with a specified communication during a specified period through application of technical means.	**No equivalent**	**Legal Analysis** There is no procedural power to collect traffic data real-time. There could be a lower threshold to collect real-time traffic data which is an essential investigative tool. There may be situations where a higher legal threshold to secure content is not made out by an applicant – but a lower threshold to secure traffic could be. For this reason, there should be a distinction between real-time collection of stored content and traffic data. There must be safeguards and requirements/ procedure to compel CSPs cooperation to collect or record content data in real-time of specific communications in Jordan **Gap Analysis** **Recommendations:** There should be a specific power to collect traffic data real-time and provision should be made to compel CSPs in Jordan to cooperate with real-time collection of traffic data; and safeguards should be incorporated to ensure the collection is legal, necessary, reasonable and proportionate in the circumstances. The language from Article 28 CITO could be considered but this does not refer to real-time only expeditious collection. Article 20 BC and section 25 HIPCAR should be used as a guide for national legislation

Procedure

International Best Practice	National Legislation	Comments
3.A country may decide not to implement section 25.		
		Disclosure obligation of encryption keys With terrorists and organized criminals routinely using encrypted messaging applications229 this may be considered a viable power to release the keys to passwords to unlock devices[230] **Gap Analysis** **Recommendation:** Unable to clarify if such powers in Jordan – this will allow law enforcement to compel owners to unlock devices
		Data retention obligations[231] Such a power can allow law enforcement to 1. Trace and identify the source of a communication 2. Identify the destination of a communication; 3. Identify the date, time and duration of a communication; and 4. Identify the type of communication Jordan does not have such an obligation[232]

International Cooperation

International Best Practice	National Legislation	Comments
Article 22 BC **Jurisdiction** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:	**No equivalent**	**Legal Analysis** Without a clearly defined scope for cybercrime offences, that are international in nature, any legislation will be restricted.

229. Eleanor Saitta. "Can Encryption Save Us?" Nation 300, no. 24 (June 15, 2015): 16-18. Academic Search Premier, EBSCOhost (accessed February 29, 2016).

230. For an example see section 49 Regulation of Investigatory Powers Act 2000 (UK) - http://www.legislation.gov.uk/ukpga/2000/23/section/49

231. In 2006 under the Data Retention Directive - EU Member States had to store electronic telecommunications data for at most 6 months for investigating, detecting and prosecuting serious crime. In 2014, the Court of Justice of the EU invalidated the Data Retention Directive, holding that it provided insufficient safeguards against interferences with the rights to privacy and data protection. For national schemes see: http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention

232. ICMEC Global Review page 29

International Cooperation		
International Best Practice	National Legislation	Comments
a. in its territory; or b. on board a ship flying the flag of that Party; or c. on board an aircraft registered under the laws of that Party; or d. by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. 2. Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 3. Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition. 4. This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. 5. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.		**Gap Analysis** **Recommendation:** National legislation ensures jurisdiction is defined using the language of Article 22 BC, section 19 HIPCAR or Article 30 CITO. If there is a conflict between jurisdictions consideration should be given to guidelines on determining the appropriate jurisdiction to try an offence – see the Eurojust Guidelines for Deciding which Jurisdiction should Prosecute (revised 2016)[233]

[233] http://www.eurojust.europa.eu/Practitioners/operational/Documents/Operational-Guidelines-for-Deciding.pdf

International Cooperation		
International Best Practice	National Legislation	Comments
Section 19 HIPCAR – Jurisdiction This Act applies to an act done or an omission made: • in the territory of [enacting country]; or • on a ship or aircraft registered in [enacting country]; or • by a national of [enacting country] outside the jurisdiction of any country; or by a national of [enacting country] outside the territory of [enacting country], if the person's conduct would also constitute an offence under a law of the country where the offence was committed. **Article 30 CITO - Competence** 1. Every State Party shall commit itself to adopting the procedures necessary to extend its competence to any of the offences set forth in Chapter II of this Convention, if the offence is committed, partly or totally, or was realized: a. in the territory of the State Party b. on board a ship raising the flag of the State Party. c. on board a plane registered under the law of the State Party. d. by a national of the State Party if the offence is punishable according to the domestic law in the location where it was committed, or if it was committed outside the jurisdiction of any State. e. If the offence affects an overriding interest of the State.		

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
2. Every State Party shall commit itself to adopting the procedures necessary to extend the competence covering the offences set forth in Article 31, paragraph 1, of this Convention in the cases in which the alleged offender is present in the territory of that State Party and shall not extradite him to another Party according to his nationality following the extradition request. 3. If more than one State Party claim to have jurisdiction over an offence set forth in this Convention, priority shall be accorded to the request of the State whose security or interests were disrupted by the offence, followed by the State in whose territory the offence was committed, and then by the State of which the wanted person is a national. In case of similar circumstances, priority shall be accorded to the first State that requests the extradition.		
Article 43 CITO **Specialized Body**[234] 1. Every State Party shall guarantee, according to the basic principles of its legal system, the presence of a specialized body dedicated 24 hours a day to ensure the provision of prompt assistance for the purposes of investigation, procedures related to information technology offences or gather evidence in electronic form regarding a specific offence. Such assistance shall involve facilitating or implementing: a. provision of technical advice.	**No equivalent**	**Legal Analysis** This is an essential mechanism for an effective cybercrime investigative capability. **Gap Analysis** **Recommendation:** This should not require legislation to implement and subject to resources should be established as a priority. Contact details should be shared for the nominated single point of contact (SPOC) nationally, central authorities internationally and INTERPOL. Consideration should also be given to drafting a Memorandum of Understanding with national agencies so that the SPOC has authority to undertake the actions required as part of an international cybercrime investigation applying national laws and treaties. This MOU will include both incoming and outgoing requests and ensure an efficient and effective process.

[234] Article 35 BC

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
b. safeguarding information based on Articles 37 and 38. c. collecting evidence, provide legal information and locate suspects. 2. a. In all State Parties, such a body shall be able to communicate promptly with the corresponding body in any other State Party b. If the said body, designated by a State Party, is not part of the authorities of that State Party responsible for international bilateral assistance, that body shall ensure its ability to promptly coordinate with those authorities. 3. Every State Party shall ensure the availability of capable human resources to facilitate the work of the above mentioned body.		
Article 25 BC **General principles relating to mutual assistance** 1. The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. 2. Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.		**Legal Analysis** Article 32 CITO ensures that it can be used as an instrument to facilitate MLA and provides for expedited preservation of stored computer data,[235] expedited preservation and partial disclosure of traffic data[236] and disclosure of stored data[237] and traffic data[238] to CITO states **Gap Analysis** **Recommendation:** *I*t is advisable to legislate for the procedural powers in CITO nationally in order that they can be used for domestic investigations and further are reciprocal powers to use for states not a party to CITO CITO does not provide for real-time content and traffic data interception – this should be considered applying precedents in BC and HIPCAR.[239]

[235] Article 29 BC and Article 37 CITO

[236] Article 30 BC and Article 38 CITO

[237] Article 31 BC and Article 39 CITO

[238] Article 33 BC and Article 41 CITO

[239] Article 33 and 34 BC and sections 25 and 26 HIPCAR

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
3. Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication. 4. Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence. 5. Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.		Consideration should be given to allowing adjudicating authorities to authorise domestic law enforcement to investigate in the State where access to a device is known. Accessibility of information is the essential criterion to initiate an investigation in cases where it is not possible to know where the data is stored (i.e. in the cloud). This could include a "*mutual recognition*" of court orders issued towards communication service providers in a given State, that could be served to branches of that CSPs located in other States, depending on where the data is stored.

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
Article 34 CITO - Procedures for Cooperation and Mutual Assistance Requests 1. The provisions of paragraphs 2-9 of this Article shall apply in case no cooperation and mutual assistance treaty or convention exists on the basis of the applicable legislation between the State Parties requesting assistance and those from which assistance is requested. If such a treaty or convention exists, the mentioned paragraphs shall not apply, unless the concerned parties agree to apply them in full or in part. 2. a. Every State Party shall designate a central authority responsible for sending and responding to mutual assistance requests and for their implementation and referral to the relevant authorities for implementation. b. Central authorities shall communicate directly among themselves. c. Every State Party shall, at the time of signature or deposit of the instrument of ratification, acceptance or agreement, contact the General Secretariat of the Council of Arab Interior Ministers and the Technical Secretariat of the Arab Justice Ministers and communicate to them the names and addresses of the authorities specifically designated for the purposes of this paragraph.		

International Cooperation		
International Best Practice	National Legislation	Comments
d. The General Secretariat of the Council of Arab Interior Ministers and the Technical Secretariat of the Arab Justice Ministers shall establish and update a registry of concerned central authorities appointed by the State Parties. Every State Party shall insure that the registry's details are correct at all times 3. Mutual assistance requests in this Article shall be implemented according to procedures specified by the requesting State Party, except in the case of non conformity with the law of the State Party from which assistance is requested. 4. The State Party from which assistance is requested may postpone taking action on the request if such action shall affect criminal investigations conducted by its authorities. 5. Prior to refusing or postponing assistance, the State Party from which assistance is requested shall decide, after consulting with the requesting State Party, whether the request shall be partially fulfilled or be subject to whatever conditions it may deem necessary. 6. The State Party from which assistance is requested shall commit itself to inform the requesting State Party of the result of the implementation of the request. If the request is refused or postponed, the reasons of such refusal or postponement shall be given. The State Party from which assistance is requested shall inform the requesting State Party of the reasons that prevent the complete fulfilment of the request or the reasons for its considerable postponement.		

International Cooperation		
International Best Practice	National Legislation	Comments
7. The State Party requesting assistance may request the State Party from which assistance is requested to maintain the confidentiality of the nature and content of any request covered by this chapter, except in as far as necessary to implement the request. If the State Party from which assistance is requested cannot abide by this request concerning confidentiality, it shall so inform the requesting State Party which will then decide about the possibility of implementing the request. 8. a. In case of emergency, mutual assistance requests may be sent directly to the judicial authorities in the State Party from which assistance is requested from their counterparts in the requesting State Party. In such case, a copy shall be sent concurrently from the central authority in the requesting State Party to its counterpart in the State Party from which assistance is requested. b. Communications can be made and requests submitted pursuant to this paragraph through INTERPOL. c. Whenever, according to paragraph a, a request is submitted to an authority, but that authority is not competent to deal with that request, it shall refer the request to the competent authority and directly inform the requesting State Party accordingly.		

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
d. Communications and requests carried out according to this paragraph and not concerning compulsory procedures may be transmitted directly by the competent authorities in the requesting State Party to their counterpart in the State Party from which assistance is requested. e. Every State Party may, at the time of signature, ratification, acceptance or adoption, inform the General Secretariat of the Council of Arab Interior Ministers and the Technical Secretariat of the Arab Justice Ministers that requests according to this paragraph must be submitted to the central authority for reasons of efficiency.		
Article 26 BC[240] **Spontaneous Information** 1. A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.		**Legal Analysis** This is an important procedure to enable a state privy to information that will assist another state to prevent a cybercrime or to investigate it. Albeit available between CITO ratified states in CITO Article 33, Jordan has no domestic legal basis to share such information with non-CITO states unless an official request is sent through the usual MLA channels. Article 18(4)-(5) UNTOC provides for the sharing of intelligence spontaneously for matters fulfilling the definition of a serious crime[241], that is transnational[242] and involves an organized crime group[243]. Without satisfying this definition an official request will need to be sent through the usual MLA channels to non-CITO states. On the basis of the fast-moving nature of cybercriminality spontaneous sharing is an effective way to cooperate with other states and its absence inhibits effective international collaboration with non-CITO states.

[240] Article 33 CITO

[241] Article 2(b) UNTOC "*"Serious crime" shall mean conduct constituting an offence punish- able by a maximum deprivation of liberty of at least four years or a more serious penalty*"

[242] Article 3(1) UNTOC

[243] Article 2(a) UNTOC "*"Organized criminal group" shall mean a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit*"

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
2. Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them. **Article 33 CITO - Circumstantial Information** 1. A State Party may – within the confines of its domestic law – and without prior request, give another State information it obtained through its investigations if it considers that the disclosure of such information could help the receiving State Party in investigating offences set forth in this convention or could lead to a request for cooperation from that State Party. 2. Before giving such information, the State Party providing it may request that the confidentiality of the information be kept; if the receiving State Party cannot abide by this request, it shall so inform the State Party providing the information which will then decide about the possibility of providing the information. If the receiving State Party accepts the information on condition of confidentiality, the information shall remain between the two sides.	**No equivalent**	**Gap Analysis** **Recommendation:** Use UNTOC Article 18(4)-(5) as the basis to spontaneously share information that fulfils the scope of UNTOC (with guarantees provided about use in evidence or disclosure of sensitive information to a third party (including another state).[244] Consider legislation based on Article 33 CITO or Article 26 BC.

[244] See Article 33(2) CITO

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
Article 32 BC – Trans-Border A Party may, without the authorisation of another Party: a. access publicly available (open source) stored computer data, regardless of where the data is located geographically; or b. access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system. **Section 27 HIPCAR** 1. If a [judge] [magistrate] is satisfied on the basis of [information on oath] [affidavit] that in an investigation concerning an offence listed in paragraph 7 herein below there are reasonable grounds to believe that essential evidence cannot be collected by applying other instruments listed in Part IV but is reasonably required for the purposes of a criminal investigation, the [judge] [magistrate] [may] [shall] on application authorize a [law enforcement] [police] officer to utilize a remote forensic software with the specific task required for the investigation and install it on the suspect's computer system in order to collect the relevant evidence. The application needs to contain the following information:	**No equivalent**	**Legal Analysis** This procedural power enables a state to secure content stored in another state in limited circumstances. Article 32.b. BC and Article 40 CITO is an exception to the principle of territoriality and permits unilateral trans-border access without the need for mutual legal assistance where there is consent or the information is publicly available. Examples of use of this procedural power under BC Article 32.b. include: A person's e-mail may be stored in another country by a service provider, or a person may intentionally store data in another country. These persons may retrieve the data and, provided that they have the lawful authority, they may voluntarily disclose the data to law enforcement officials or permit such officials to access the data[245] A suspected terrorist is lawfully arrested while his/her mailbox – possibly with evidence of a crime – is open on his/her tablet, smartphone or other device. If the suspect voluntarily consents that the police access the account and if the police are sure that the data of the mailbox is located in another state, police may access the data under Article 32.b.

[245] Paragraph 294, page 53 BC Explanatory Report

International Cooperation		
International Best Practice	National Legislation	Comments
• suspect of the offence, if possible with name and address; and • description of the targeted computer system; and • description of the intended measure, extent and duration of the utilization; and • reasons for the necessity of the utilization. 2. Within such investigation it is necessary to ensure that modifications to the computer system of the suspect are limited to those essential for the investigation and that any changes if possible can be undone after the end of the investigation. During the investigation, it is necessary to log • the technical mean used and time and date of the application; and • the identification of the computer system and details of the modifications undertaken within the investigation; • any information obtained. Information obtained by the use of such software needs to be protected against any modification, unauthorized deletion and unauthorized access. 3. The duration of authorization in section 27 (1) is limited to [3 months]. If the conditions of the authorization is no longer met, the action taken are to stop immediately. 4. The authorization to install the software includes remotely accessing the suspects computer system. 5. If the installation process requires physical access to a place the requirements of section 20 need to be fulfilled.		**Gap Analysis** **Recommendation:** This restricted power to unilaterally secure evidence is included in legislation with safeguards to ensure the consent is lawfully obtained from the user.[246] Language can be used from Article 32 BC and Article 40 CITO. Article 32.b. has been heavily criticized and it may be considered that the consent of the state where the stored computer data is stored is obtained in addition to the user. Section 27 HIPCAR provides for forensic software and this may allow access to a computer in another state. There are a number of restrictions that requires the evidence cannot be obtained by other means, a judicial order is required, can only apply to certain offences and is for a restricted period (3 months). Consideration should also be given to consent of the other state where the forensic software may intrude.

[246] Consideration should be given to situations such as the non-availability of a user (e.g. death) and if consent can be obtained in another state

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
6. If necessary a [law enforcement] [police] officer may pursuant to the order of court granted in (1) above request that the court order an internet service provider to support the installation process. 7. [List of offences]. 8. A country may decide not to implement section 27. **Article 40 CITO - Access to Information Technology Information Across Borders** A State Party may, without obtaining an authorization from another State Party: 1. Access information technology information available to the public (open source), regardless of the geographical location of the information. 2. Access or receive – through information technology in its territory – information technology information found in the other State Party, provided it has obtained the voluntary and legal agreement of the person having the legal authority to disclose information to that State Party by means of the said information technology.		

Lebanon

Lebanon adopted the Law No. 81 relating to Electronic Transactions and Personal Data on 10 October 2018 which enterred into force in January 2019. EuroMed Justice Team endeavors to keep the information up to date and correct; however in spite of our best efforts, due to the current project limitation in time and resources an analyses of the 2018 new legal provisions will be possible in the next phase.

Offences		
International Best Practice	**National Legislation**	**Comments**
Article 2 BC – Illegal Access Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system. **Article 6 CITO – Illicit Access** 1. Illicit access to, presence in or contact with part or all of the information technology, or the perpetuation thereof. 2. The punishment shall be increased if this access, presence, contact or perpetuation leads to: a. the obliteration, modification, distortion, duplication, removal or destruction of saved data, electronic instruments and systems and communication networks, and damages to the users and beneficiaries. b. the acquirement of secret government information.		**Legal Analysis** CITO refers to *“illicit access to, presence in or contact with”* without defining what these acts mean. BC refers to *“without right”* in Article 2 on the basis the access is unauthorized. The BC Explanatory Report confirmed the derivation of *“without right”* as, *“conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law.”* The Commentary sections[247] on the HIPCAR model legislation provides an explanation as to the requirement for *“without lawful excuse or justification”* as follows, *“Access to a computer system can only be prosecuted under Section 4, if it happens “without lawful excuse or justification”. This requires that the offender acts without authority (whether legislative, executive, administrative, judicial, contractual or consensual) and the conduct is otherwise not covered by established legal defences, excuses, justifications or relevant principles. Access to a system permitting free and open access by the public or access to a system with the authorisation of the owner or other rights-holder is as a consequently not criminalised. Network administrators and security companies that test the protection of computer systems in order to identify potential gaps in security measures do not commit a criminal act.”*

[247] Page 30 Commentary Section HIPCAR Model Legislation

Offences		
International Best Practice	**National Legislation**	**Comments**
Section 4 HIPCAR – Illegal Access 1. A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, accesses the whole or any part of a computer system commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. 2. A country may decide not to criminalize the mere unauthorized access provided that other effective remedies are available. Furthermore, a country may require that the offence be committed by infringing security measures or with the intent of obtaining computer data or other dishonest intent. **Section 5 HIPCAR – Illegal Remaining** 1. A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, remains logged in a computer system or part of a computer system or continues to use a computer system commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. 2. A country may decide not to criminalize the mere unauthorized remaining provided that other effective remedies are available. Alternatively, a country may require that the offence be committed by infringing security measures or with the intent of obtaining computer data or other dishonest intent.	**No Equivalent**	CITO refers to *"illicit access to, presence in or contact with"* without defining what these acts mean – therefore, BC and HIPCAR are to be preferred. **Gap Analysis** **Recommendation:** The national legislation could incorporate relevant language from Article 2 BC/sections 4 and 5 HIPCAR to include definitions of a computer system[248] and the inclusion of programs within the definition of data as some data includes programs and other data does not. Further, to be consistent with international standards the legislation should refer to access *"without right"* rather than fraudulently. Also consider a separate offence of remaining in a computer system as per section 5 HIPCAR.

[248] See Article 1.a. BC: "*any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data*" **or** section 3(5) HIPCAR: "*a device or a group of inter-connected or related devices, including the Internet, one or more of which, pursuant to a program, performs automatic processing of data or any other function.*"

Offences		
International Best Practice	**National Legislation**	**Comments**
Article 3 BC **Illegal Interception** Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system. **Section 6 HIPCAR – Illegal Interception** 1. A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, intercepts by technical means: • any non-public transmission to, from or within a computer system; or • electromagnetic emissions from a computer system commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. 2. A country may require that the offence be committed with a dishonest intent, or in relation to a computer system that is connected to another computer system, or by circumventing protection measures implemented to prevent access to the content of non-public transmission.	**No equivalent**	**Legal Analysis** This offence is essential to prosecute transmissions of computer data to, from, or within a computer system that may be illegally intercepted to obtain information (e.g. wikileaks or Panama Papers). **Gap Analysis** **Recommendation:** Use the BC language in Article 3, HIPCAR section 6 as a guide for national legislation - the language in Article 7 CITO is appropriate – albeit there is no definition of *"information technology data"*

Offences		
International Best Practice	**National Legislation**	**Comments**
Article 7 CITO **Illicit Interception** The deliberate unlawful interception of the movement of data by any technical means, and the disruption of transmission or reception of information technology data.		
Article 4 BC **Data Interference** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm. **Section 7 HIPCAR – Illegal Data Interference** A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, does any of the following acts: • damages or deteriorates computer data; or • deletes computer data ; or • alters computer data; or • renders computer data meaningless, useless or ineffective; or • obstructs, interrupts or interferes with the lawful use of computer data; or • obstructs, interrupts or interferes with any person in the lawful use of computer data; or • denies access to computer data to any person authorized to access it;	**No equivalent**	**Legal Analysis** As above for Illicit Access there is no reference in CITO to *"without right"* and does not include suppression of computer data which is an element of phishing to obtain illegal access by installing a keylogger to obtain sensitive information.[249] **Gap Analysis** **Recommendation:** The absence of certain key elements related to this offence in CITO may be remedied using language from Article 4 BC or section 7 HIPCAR.

[249] http://www.coe.int/en/web/cybercrime/guidance-notes

Offences		
International Best Practice	**National Legislation**	**Comments**
commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. **Article 8 CITO** **Offence Against the Integrity of Data** 1. Deliberate unlawful destruction, obliteration, obstruction, modification or concealment of information technology data. 2. The Party may require that, in order to criminalize acts mentioned in paragraph 1, they must cause severe damage.		
Article 5 BC[250] **System Interference** Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data. **Section 9 HIPCAR – Illegal System Interference** 1. A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification: • hinders or interferes with the functioning of a computer system; or • hinders or interferes with a person who is lawfully using or operating a computer system;	**No equivalent**	**Legal Analysis** This offence would prevent malware that interferes with the functioning of a computer – for example computer worms - a subgroup of malware (like computer viruses). They are self-replicating computer programs that harm the network by initiating multiple data-transfer processes. They can influence computer systems by hindering the smooth running of the computer system, using system resources to replicate themselves over the Internet or generating network traffic that can close down availability of certain services (such as websites).

[250] no equivalent in CITO

Offences		
International Best Practice	National Legislation	Comments
commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. 2. A person who intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification hinders or interferes with a computer system that is exclusively for the use of critical infrastructure operations, or in the case in which such is not exclusively for the use of critical infrastructure operations, but it is used in critical infrastructure operations and such conduct affects that use or impacts the operations of critical infrastructure the punishment shall be imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.		**Gap Analysis** **Recommendation:** Use the BC language in Article 5 or section 9 HIPCAR as a guide for national legislation. Also consider whether the prevention and prosecution of attacks against critical infrastructure needs a separate or aggravated offence (Section 9(2) HIPCAR) for example the functioning of a computer system may be hindered for terrorist purposes (e.g. hindering the system that stores stock exchange records can make them inaccurate, or hindering the functioning of critical infrastructure).[251]
Article 6 BC[252] **Misuse of Devices** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a. the production, sale, procurement for use, import, distribution or otherwise making available of: i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;	**No equivalent**	**Legal Analysis** As above for Illicit Access there is no reference to *"without right"* This offence will enable prosecution for the production, sale, procurement for use, import, distribution of access codes and other computerized data used to commit cybercrimes - for example computer systems may be accessed to facilitate a terrorist attack by interfering with a country's electrical power grid. Any offence would also have to consider those devices that have a legitimate as well as being put to criminal use (*"dual use"*) – this should include the BC language of *"primarily adapted"*

[251] http://www.coe.int/en/web/cybercrime/guidance-notes

[252] Article 9 CITO

Offences		
International Best Practice	**National Legislation**	**Comments**
ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b. the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3. Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article		**Gap Analysis** **Recommendation:** Use the BC language in Article 6 or section 10 HIPCA as a guide for national legislation. Please note that HIPCAR provides the option of listing the devices in a schedule if deemed appropriate – this could be restrictive and require updating with technological progress. The national law should provide a reasonable excuse so law enforcement can use devices for special investigation techniques – see the language at Article 6.2. BC or section 10(2) HIPCAR as a guide.

Offences		
International Best Practice	**National Legislation**	**Comments**
Section 10 HIPCAR – Illegal Devices 1. A person commits an offence if the person: a. intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, produces, sells, procures for use, imports, exports, distributes or otherwise makes available: i. a device, including a computer program, that is designed or adapted for the purpose of committing an offence defined by other provisions of Part II of this law; or ii. a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed; with the intent that it be used by any person for the purpose of committing an offence defined by other provisions of Part II of this law; or b. has an item mentioned in subparagraph (i) or (ii) in his or her possession with the intent that it be used by any person for the purpose of committing an offence defined by other provisions of part II of this law commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.		

Offences		
International Best Practice	**National Legislation**	**Comments**
2. This provision shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 is not for the purpose of committing an offence established in accordance with other provisions of Part II of this law, such as for the authorized testing or protection of a computer system. 3. A country may decide not to criminalize illegal devices or limit the criminalization to devices listed in a Schedule.		
Article 7 BC **Computer Related Forgery** Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches. **Article 10 CITO** **Offence of Forgery** The use of information technology means to alter the truth of data in a manner that causes harm, with the intent of using them as true data.	**No equivalent**	**Legal Analysis** Any offence of forgery is prosecuted as a substantive offence only – the purpose of Article 7 BC is to fil gaps in criminal law related to traditional forgery, which requires visual readability of statements, or declarations embodied in a document and which does not apply to electronically stored data. Computer-related forgery involves unauthorised creating or altering stored data so that they acquire a different evidentiary value in the course of legal transactions, which relies on the authenticity of information contained in the data, is subject to a deception. The protected legal interest is the security and reliability of electronic data which may have consequences for legal relations.[253] Incorporation of BC article 7 or section 11 HIPCAR is advised to protect against this offending which could include phishing and spear phishing For example, computer data (such as the data used in electronic passports) may be input, altered, deleted, or suppressed with the result that inauthentic data is considered or acted upon for legal purposes as if it were authentic.[254]

[253] Paragraph 81, page 14 Explanatory Report BC

[254] http://www.coe.int/en/web/cybercrime/guidance-notes

Offences		
International Best Practice	**National Legislation**	**Comments**
Section 11 HIPCAR – Computer-related Forgery 1. A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification inputs, alters, deletes, or suppresses computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. 2. If the abovementioned offence is committed by sending out multiple electronic mail messages from or through computer systems, the penalty shall be imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.		Section 11(2) HIPCAR also provides for the sending of multiple electronic email messages as an aggravated offence. The language in Article 10 CITO has no reference to any dishonest intent and requires harm to be caused – the language in BC and HIPCAR is to be preferred as it does not require harm to be caused. BC and HIPCAR only requires that the "*inauthentic data*" data is "*considered*" **Gap Analysis** **Recommendation:** Use the BC language in Article 7 or section 11 HIPCAR as a guide for national legislation
Article 8 BC[255] **Computer Related Fraud** Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a. any input, alteration, deletion or suppression of computer data, b. any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneselfor for another person.		**Legal Analysis** Any offence of fraud is prosecuted as a substantive offence. Computer related fraud consist mainly of input manipulations, where incorrect data is fed into the computer, or by programme manipulations and other interferences with the course of data processing.The aim of Article 8 is to criminalise any undue manipulation in the course of data processing with the intention to effect an illegal transfer of property.[256] The language in Article 11 CITO is vague with no reference to any dishonest intent and requires some form of *"harm"* (CITO) without defining what this is **Gap Analysis** **Recommendation:** The language in BC or HIPCAR for this offence is a good guide for national legislation

[255] Article 11 CITO

[256] Paragraph 86, pages 14 and 15 Explanatory Report BC

Offences		
International Best Practice	**National Legislation**	**Comments**
Article 8 BC[257] **Computer Related Fraud** Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: c. any input, alteration, deletion or suppression of computer data, d. any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneselfor for another person. **Section 12 HIPCAR – Computer-related Fraud** A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification causes a loss of property to another person by: • any input, alteration, deletion or suppression of computer data; • any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person the penalty shall be imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.	**No equivalent**	

[257] Article 11 CITO

Offences		
International Best Practice	**National Legislation**	**Comments**
Article 9 BC **Content related offences (e.g. child pornography)** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a. producing child pornography for the purpose of its distribution through a computer system; b. offering or making available child pornography through a computer system; c. distributing or transmitting child pornography through a computer system; d. procuring child pornography through a computer system for oneself or for another person; e. possessing child pornography in a computer system or on a computer-data storage medium. 2. For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: a. a minor engaged in sexually explicit conduct; b. a person appearing to be a minor engaged in sexually explicit conduct; c. realistic images representing a minor engaged in sexually explicit conduct. 3. For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.	**No equivalent**	**Legal Analysis** This is an essential offence in order to protect children from harm by criminalizing the distribution, transmitting, making available, offering, producing and possession of indecent images of children. **Gap Analysis** **Recommendation:** The language in BC Article 9 or section 13 HIPCAR is a guide for national legislation to protect children and prosecute perpetrators

Offences		
International Best Practice	**National Legislation**	**Comments**
4. Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c. **Section 13 HIPCAR – Child Pornography** 1. A person who, intentionally, without lawful excuse or justification: • produces child pornography for the purpose of its distribution through a computer system; • offers or makes available child pornography through a computer system; • distributes or transmits child pornography through a computer system; • procures and/or obtain child pornography through a computer system for oneself or for another person; • Possesses child pornography in a computer system or on a computer- data storage medium; or • knowingly obtains access, through information and communication technologies, to child pornography, commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. 2. It is a defense to a charge of an offence under paragraph (1) (b) to (1)(f) if the person establishes that the child pornography was a bona fide law enforcement purpose. 3. A country may not criminalize the conduct described in section 13 (1) (d)- (f).		

Offences		
International Best Practice	**National Legislation**	**Comments**
Article 10 BC **Infringement of copyright** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.	**No equivalent**	**Legal Analysis** Law enforcement internationally utilizes digital copyright offences as additional criminal conduct to investigate and prosecute several forms of cybercrime (which include crimes such as phishing, electronic fraud, electronic forgery, fraudulent websites and data theft/data breaches). One of the underlying offences in many of these cases tends to be infringement of digital copyright. The Sony cyber-attack[258] is only one recent example where offences and powers related to cybercrime, data theft/corporate espionage and copyright infringement came together to complement one another. The absence of any provisions relating to intellectual property would constitute a failure to protect the innovation in the 21st century of the SPCs, businesses and citizens. This may of course be protected in other legislation not reviewed as part of this analysis **Gap Analysis** **Recommendation:** Ensure that there are protections against infringement of copyright that comply with international obligations.

[258] https://en.wikipedia.org/wiki/Sony_Pictures_hack

Offences		
International Best Practice	**National Legislation**	**Comments**
3. A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article. **Article 17 CITO - Offenses Related to Copyright and Adjacent Rights** Violation of copyright as defined according to the law of the State Party, if the act is committed deliberately and for no personal use, and violation of rights adjacent to the relevant copyright as defined according to the law of the State Party, if the act is committed deliberately and for no personal use.		

Offences		
International Best Practice	**National Legislation**	**Comments**
Article 11 BC **Aiding and Abetting** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed. 2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention. **Article 19 CITO - Attempt at and Participation in the Commission of Offences** 1. Participation in the commission of any of the offences set forth in this chapter with the intention to commit the offence in the law of the State Party. 2. Attempt at the commission the offences set forth in Chapter II of this convention. 3. A State Party may reserve the right to not implement the second paragraph of this Article totally or partly.	**No equivalent**	**Legal Analysis** Aiding and abetting others to commit offences is essential in order to prosecute those who may have provided assistance or encouraged cybercrimes to take place. Article 19 CITO also includes attempt **Gap Analysis** Recommendation: Use Article 11 BC and Article 19 CITO as a guide for national legislation

Offences		
International Best Practice	**National Legislation**	**Comments**
Article 12 BC[259] **Corporate liability** 1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on: a. a power of representation of the legal person; b. an authority to take decisions on behalf of the legal person; c. an authority to exercise control within the legal person. 2. In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority. 3. Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative. 4. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.	**No equivalent**	**Legal Analysis** This provision is an essential element so that legal persons (e.g. corporate entities) acting on behalf of natural persons have criminal liability **Gap Analysis** **Recommendation:** Use the BC language in Article 12 as a guide for national legislation

[259] Article 20 CITO

Offences		
International Best Practice	**National Legislation**	**Comments**
Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems **Article 3[260] – Dissemination of racist and xenophobic material through computer systems** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: distributing, or otherwise making available, racist and xenophobic material to the public through a computer system. 2. A Party may reserve the right not to attach criminal liability to conduct as defined by paragraph 1 of this article, where the material, as defined in Article 2, paragraph 1, advocates, promotes or incites discrimination that is not associated with hatred or violence, provided that other effective remedies are available. 3. Notwithstanding paragraph 2 of this article, a Party may reserve the right not to apply paragraph 1 to those cases of discrimination for which, due to established principles in its national legal system concerning freedom of expression, it cannot provide for effective remedies as referred to in the said paragraph 2.	**No equivalent**	**Gap Analysis** **Recommendation:** Use the BC language in Article 3 Additional Protocol as a guide for national legislation

[260] no equivalent in CITO

Offences		
International Best Practice	**National Legislation**	**Comments**
Additional Protocol **Article 4[261] – Racist and xenophobic motivated threat** Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: threatening, through a computer system, with the commission of a serious criminal offence as defined under its domestic law, (i) persons for the reason that they belong to a group, distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors, or (ii) a group of persons which is distinguished by any of these characteristics.	**No equivalent**	**Gap Analysis** **Recommendation:** Use the BC language in Article 4 Additional Protocol as a guide for national legislation
Additional Protocol **Article 5[262] - Racist and xenophobic motivated insult** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: insulting publicly, through a computer system, (i) persons for the reason that they belong to a group distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors; or (ii) a group of persons which is distinguished by any of these characteristics.	**No equivalent**	**Gap Analysis** **Recommendation:** Use the BC language in Article 5 Additional Protocol as a guide for national legislation

[261] no equivalent in CITO
[262] no equivalent in CITO

Offences		
International Best Practice	**National Legislation**	**Comments**
2. A Party may either: a. require that the offence referred to in paragraph 1 of this article has the effect that the person or group of persons referred to in paragraph 1 is exposed to hatred, contempt or ridicule; or b. reserve the right not to apply, in whole or in part, paragraph 1 of this article.		
Additional Protocol **Article 6[263] - Denial, gross minimisation, approval or justification of genocide or crimes against humanity** 1. Each Party shall adopt such legislative measures as may be necessary to establish the following conduct as criminal offences under its domestic law, when committed intentionally and without right: distributing or otherwise making available, through a computer system to the public, material which denies, grossly minimises, approves or justifies acts constituting genocide or crimes against humanity, as defined by international law and recognised as such by final and binding decisions of the International Military Tribunal, established by the London Agreement of 8 August 1945, or of any other international court established by relevant international instruments and whose jurisdiction is recognised by that Party.	**No equivalent**	**Gap Analysis** **Recommendation:** Use the BC language in Article 6 Additional Protocol as a guide for national legislation

[263] no equivalent in CITO

Offences		
International Best Practice	**National Legislation**	**Comments**
2. A Party may either a. require that the denial or the gross minimisation referred to in paragraph 1 of this article is committed with the intent to incite hatred, discrimination or violence against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors, or otherwise b. reserve the right not to apply, in whole or in part, paragraph 1 of this article.		
Additional Offences to Review		
Identity-related Crimes **Section 14 HIPCAR** A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification by using a computer system in any stage of the offence, intentionally transfers, possesses, or uses, without lawful excuse or justification, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a crime, commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.		**Legal Analysis** This offence covers the preparation phase of an identity –related crime of dishonesty **Gap Analysis** **Recommendation:** Inclusion in domestic legislation is advisable.

Offences

International Best Practice	National Legislation	Comments
Disclosure of Details of an Investigation **Section 16 HIPCAR** An Internet service provider who receives an order related to a criminal investigation that explicitly stipulates that confidentiality is to be maintained or such obligation is stated by law and intentionally without lawful excuse or justification or in excess of a lawful excuse or justification discloses: • the fact that an order has been made; or • anything done under the order; or • any data collected or recorded under the order; commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.		**Legal Analysis** This offence sanctions data breaches and disclosure of sensitive information that could impact criminal investigations **Gap Analysis** **Recommendation:** Inclusion in domestic legislation is advisable.
Failing to Permit Assistance **Section 17 HIPCAR** 1. A person other than the suspect who intentionally fails without lawful excuse or justification or in excess of a lawful excuse or justification to permit or assist a person based on an order as specified by sections 20 to 22[264] commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. 2. A country may decide not to criminalize the failure to permit assistance provided that other effective remedies are available.		**Legal Analysis** This offence relates to persons, with specific knowledge of relevant evidence, who refuse to assist. Often law enforcement will be reliant upon such persons to secure evidence in cyber investigations. A separate offence is the failure to provide passwords or access to codes to encrypted devices or data (i.e. *"key to protected information"*) – section 53 of the UK Regulation of Investigatory Powers Act 2000 (RIPA) [265] provides for a criminal offence for persons who fail to comply with a section 49 RIPA Notice to disclose the *"key"* **Gap Analysis** **Recommendation:** Inclusion in domestic legislation is advisable.

[264] Search and seizure, assistance and production orders

[265] http://www.legislation.gov.uk/ukpga/2000/23/section/53

Offences		
International Best Practice	**National Legislation**	**Comments**
Cyber Stalking **Section 18 HIPCAR** A person, who without lawful excuse or justification or in excess of a lawful excuse or justification initiates any electronic communication, with the intent to coerce, intimidate, harass, or cause substantial emotional distress to a person, using a computer system to support severe, repeated, and hostile behavior, commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.		**Legal Analysis** This offence criminalizes those who harass persons online– some jurisdictions may have non-computer related harassment offences – but this offence is recommended for those crimes committed online. **Gap Analysis** **Recommendation:** Inclusion in domestic legislation is advisable.
Grooming Children Online **Dutch Criminal Code 248e** The person who proposes to arrange a meeting, by means of an automated work or by making use of a communication service, to a person of whom he knows, or should reasonably assume, that such person has not yet reached the age of sixteen, with the intention of committing indecent acts with this person or of creating an image of a sexual act in which this person is involved, will be punished with a term of imprisonment of at most two years or a fine of the fourth category, if he undertakes any action intended to realise that meeting. **Canadian Criminal Code** **Section 172.1** 1. Every person commits an offence who, by a means of telecommunication, communicates with a. a person who is, or who the accused believes is, under the age of 18 years, for the purpose of facilitating the commission of an offence under subsection 153(1), section 155, 163.1, 170 or 171 or subsection 212(1), (2), (2.1) or (4) with respect to that person;		**Legal Analysis** To prove the Dutch offence a meeting for sexual purposes is required with supporting evidence of online chat history with sexual intent; request for a meeting with evidence this was planned (i.e. date and place). The purpose of the Canadian law is to prevent grooming by predatory adults of children online. This offence does not require the sexual offence to have occurred. This means the accused does not need to have actually gone to meet the victim in person. The offence is committed before any actions are taken to commit the substantive offence. **Gap Analysis** **Recommendation:** Inclusion in domestic legislation is advisable to criminalise this preparatory behaviour before a sexual offence is committed

Offences		
International Best Practice	**National Legislation**	**Comments**
b. a person who is, or who the accused believes is, under the age of 16 years, for the purpose of facilitating the commission of an offence under section 151 or 152, subsection 160(3) or 173(2) or section 271, 272, 273 or 280 with respect to that person; or c. a person who is, or who the accused believes is, under the age of 14 years, for the purpose of facilitating the commission of an offence under section 281 with respect to that person. Punishment 2. Every person who commits an offence under subsection (1) is guilty of a. is guilty of an indictable offence and is liable to imprisonment for a term of not more than 10 years and to a minimum punishment of imprisonment for a term of one year; or b. is guilty of an offence punishable on summary conviction and is liable to imprisonment for a term of not more than 18 months and to a minimum punishment of imprisonment for a term of 90 days. Presumption re age 3. Evidence that the person referred to in paragraph (1)(a), (b) or (c) was represented to the accused as being under the age of eighteen years, sixteen years or fourteen years, as the case may be, is, in the absence of evidence to the contrary, proof that the accused believed that the person was under that age.		

Offences

International Best Practice	National Legislation	Comments
No defence 4. It is not a defence to a charge under paragraph (1)(a), (b) or (c) that the accused believed that the person referred to in that paragraph was at least eighteen years of age, sixteen years or fourteen years of age, as the case may be, unless the accused took reasonable steps to ascertain the age of the person.		

Procedure

International Best Practice	National Legislation	Comments
Article 19 BC **Search and seizure of stored computer data** 1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a. a computer system or part of it and computer data stored therein; and b. a computer-data storage medium in which computer data may be stored in its territory. 2. Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.	**No equivalent**	**Legal Analysis** This is the most essential investigatory power and should refer to gaining access than search. In the BC Explanatory Report, *"Search"* means to seek, read, inspect or review data. It includes the notion of searching for data and searching of (examining) data. The word *"access"* has a neutral meaning and reflects more accurately computer terminology – further this is used in Articles 26 and 27 CITO.[266]

[266] Paragraph 191, page 33 Explanatory Report BC

Procedure		
International Best Practice	**National Legislation**	**Comments**
3. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a. seize or similarly secure a computer system or part of it or a computer-data storage medium; b. make and retain a copy of those computer data; c. c maintain the integrity of the relevant stored computer data; d. d render inaccessible or remove those computer data in the accessed computer system. 4. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2. 5. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.		**Gap Analysis** **Recommendation:** The national legislation could incorporate relevant language from BC and HIPCAR to include definitions of a *computer system*[267] and *computer data*[268] There should be a definition of "*seize*" to insure integrity and to specific procedures - section 3(16) HIPCAR "*Seize includes:* • *activating any onsite computer system and computer data storage media;* • *making and retaining a copy of computer data, including by using onsite equipment;* • *maintaining the integrity of the relevant stored computer data;* • *rendering inaccessible, or removing, computer data in the accessed computer system;* • *taking a printout of output of computer data; or* • *seize or similarly secure a computer system or part of it or a computer- data storage medium.*" Section 21 HIPCAR provides for legislation to ensure assistance is provided by those who have specialist knowledge of the location of relevant evidence – this could be used as a guide – also see section 17 HIPCAR for an offence if assistance is refused without lawful excuse

[267] See Article 1.a. BC: "*any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data*" **or** section 3(5) HIPCAR: "*a device or a group of inter-connected or related devices, including the Internet, one or more of which, pursuant to a program, performs automatic processing of data or any other function.*"

[268] See Article 1.b. BC: "*any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function*" **or** section 3(6) HIPCAR: "*Computer data means any representation of facts, concepts, information (being either texts, sounds or images) machine-readable code or instructions, in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.*"

Procedure		
International Best Practice	**National Legislation**	**Comments**
Section 20 HIPCAR – Search and Seizure 1. If a [judge] [magistrate] is satisfied on the basis of [information on oath] [affidavit] that there are reasonable grounds [to suspect] [to believe] that there may be in a place a thing or computer data: • that may be material as evidence in proving an offence; or • that has been acquired by a person as a result of an offence; the [judge] [magistrate] [may] [shall] issue a warrant authorizing a [law enforcement] [police] officer, with such assistance as may be necessary, to enter the place to search and seize the thing or computer data including search or similarly access: i. a computer system or part of it and computer data stored therein; and ii. a computer-data storage medium in which computer data may be stored in the territory of the country. 2. If [law enforcement] [police] officer that is undertaking a search based on Sec. 20 (1) has grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, he shall be able to expeditiously extend the search or similar accessing to the other system.		

Procedure		
International Best Practice	**National Legislation**	**Comments**
3. A [law enforcement] [police] officer that is undertaking a search are empowered to seize or similarly secure computer data accessed according to paragraphs 1 or 2. **Section 21 HIPCAR – Assistance** Any person who is not a suspect of a crime but who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein that is the subject of a search under section 20 must permit, and assist if reasonably required and requested by the person authorized to make the search by: • providing information that enables the undertaking of measures referred to in section 20; • accessing and using a computer system or computer data storage medium to search any computer data available to or in the system; • obtaining and copying such computer data; • using equipment to make copies; and • obtaining an intelligible output from a computer system in such a format that is admissible for the purpose of legal proceedings. **Article 26 CITO - Inspecting Stored Information** 1. Every State Party shall commit itself to adopting the procedures necessary to enable its competent authorities to inspect or access: a. an information technology or part thereof and the information stored therein or thereon.		

Procedure		
International Best Practice	National Legislation	Comments
b. the storage environment or medium in or on which the information may be stored. 2. Every State Party shall commit itself to adopting the procedures necessary to enable the competent authorities to inspect or access a specific information technology or part thereof in conformity with paragraph 1(a) if it is believed that the required information is stored in another information technology or in part thereof in its territory and such information is legally accessible or available in the first technology, the scope of inspection may be extended and the other technology accessed. **Article 27 CITO - Seizure of Stored Information** 1. Every State Party shall commit itself to adopting the procedures necessary to enable the competent authorities to seize and safeguard information technology information accessed according to Article 26, paragraph 1, of this Convention. These procedures include the authority to: a. seize and safeguard the information technology or part thereof or the storage medium for the information technology information. b. make a copy the information technology information and keep it. c. maintain the integrity of the stored information technology information. d. remove such accessed information from the information technology or prevent its access.		

Procedure		
International Best Practice	**National Legislation**	**Comments**
2. Every State Party shall commit itself to adopting the procedures necessary to enable the competent authorities to order any person who is acquainted with the functioning of the information technology or the procedures applied to protect the information technology to give the information necessary to complete the procedures mentioned in paragraphs 2 and 3 of Article 26 of this Convention.		
Article 16 BC **Expedited preservation of stored computer data** 1. Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.	**No equivalent**	**Legal Analysis** This procedural power is important to ensure that data which is vulnerable to deletion or loss is preserved. Although no provision has been provided to preserve – the questionnaire confirms that any reqest for preservation should be sent to The Prosecutor General's Office near the Court of Cassation. **Gap Analysis** **Recommendation:** This expedited power to retain BSI, metadata, transactional and stored content is essential as part of cybercrime investigations to ensure the evidence is available for search, access, seizure and review. The language of Article 16 of the BC, section 23 HIPCAR or Article 23 CITO could be used. This will also require definitions of *"computer data"*,[269] *"subscriber information or BSI"*, *"traffic data"*[270] and *"Communication Service Provider"*[271] To note BC and HIPCAR do not provide a definition of BSI – but CITO does for subscriber information:[272]

[269] See Article 1.b. BC **or** section 3(6) HIPCAR

[270] See Article 1.d BC: "*any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service*" **or** section 3(18) HIPCAR: "*Traffic data means computer data that: a. relates to a communication by means of a computer system; and b. is generated by a computer system that is part of the chain of communication ; and c. shows the communication's origin, destination, route, time date, size, duration or the type of underlying services.*"

[271] See Article 1.c. BC: "*i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii any other entity that processes or stores computer data on behalf of such communication service or users of such service.*"

[272] See Article 2(9) CITO

Procedure		
International Best Practice	**National Legislation**	**Comments**
2. Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 3. Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. 4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15. **Section 23 HIPCAR – Expedited Preservation** If a [law enforcement] [police] officer is satisfied that there are grounds to believe that computer data that is reasonably required for the purposes of a criminal investigation is particularly vulnerable to loss or modification, the [law enforcement] [police] officer may, by written notice given to a person in control of the computer data, require the person to ensure that the data specified in the notice be preserved for a period of up to seven (7) days as specified in the notice. The period may be extended beyond seven (7) days if, on an ex parte application, a [judge] [magistrate] authorizes an extension for a further specified period of time.		*"Any information that the service provider has concerning the subscribers to the service, except for information through which the following can be known:* a. *The type of communication service used, the technical requirements and the period of service.* b. *The identity of the subscriber, his postal or geographic address or phone number and the payment information available by virtue of the service agreement or arrangement* c. *Any other information on the installation site of the communication equipment by virtue of the service agreement."* Consideration should be given the length of preservation that is reasonable in the circumstances and allowing for an application to extend in exigent circumstances – BC and CITO have 90 days and HIPCAR 7 days. From experience 90 days is too few in a cyber investigation and the figure should be nearer 180 days and then subject to extension.

Procedure		
International Best Practice	**National Legislation**	**Comments**
Article 23 CITO - Expeditious Custody of Data Stored in Information Technology 1. Every State Party shall adopt the procedures necessary to enable the competent authorities to issue orders or obtain the expeditious custody of information, including information for tracking users, that was stored on an information technology, especially if it is believed that such information could be lost or amended. 2. Every State Party shall commit itself to adopting the procedures necessary as regards paragraph 1, by means of issuing an order to a person to preserve the information technology information in his possession or under his control, in order to require him to preserve and maintain the integrity of such information for a maximum period of 90 days that may be renewed, in order to allow the competent authorities to search and investigate 3. Every State Party shall commit itself to adopting the procedures necessary to require the person responsible for safeguarding the information technology to maintain the procedures secrecy throughout the legal period stated in the domestic law.		
Article 17 BC **Expedited preservation and partial disclosure of traffic data** 1. Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:	**No equivalent**	**Legal Analysis** This procedural power is especially important to ensure that CSPs provide IP addresses that could locate the perpetrator of a cybercrime.

Procedure		
International Best Practice	**National Legislation**	**Comments**
a. ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and b. ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted. 2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15. **Section 23 HIPCAR – Expedited Preservation** If a [law enforcement] [police] officer is satisfied that there are grounds to believe that computer data that is reasonably required for the purposes of a criminal investigation is particularly vulnerable to loss or modification, the [law enforcement] [police] officer may, by written notice given to a person in control of the computer data, require the person to ensure that the data specified in the notice be preserved for a period of up to seven (7) days as specified in the notice.The period may be extended beyond seven (7) days if, on an ex parte application, a [judge] [magistrate] authorizes an extension for a further specified period of time.		**Gap Analysis** **Recommendation:** This expedited power alongside disclosure of traffic data should be included in legislation to enable effective investigations of cybercrime.The language of Article 17 of the BC, sections 23 and 24 HIPCAR or Article 24 CITO could be used. This will also require definitions of *"traffic data" and "Communication Service Provider"*[273]

[273] See definitions above

Procedure		
International Best Practice	**National Legislation**	**Comments**
Section 24 HIPCAR – Partial Disclosure of Traffic Data 1. If a [law enforcement] [police] officer is satisfied that data stored in a computer system is reasonably required for the purposes of a criminal investigation, the [law enforcement] [police] officer may, by written notice given to a person in control of the computer system, require the person to disclose sufficient traffic data about a specified communication to identify: a. the Internet service providers; and/or b. the path through which the communication was transmitted. **Article 24 CITO - Expeditious Custody and Partial Disclosure of Users Tracking Information** Every State Party shall commit itself to adopting the procedures necessary as regards users tracking information in order to: 1. ensure expeditious custody of users tracking information, regardless of whether such communication is transmitted by one or more service providers. 2. ensure that a sufficient amount of users tracking information is disclosed to the competent authorities of the State Party or to a person appointed by these authorities to allow the State Party to determine the service providers and the transmission path of the communications.		

Procedure		
International Best Practice	**National Legislation**	**Comments**
Article 18 BC **Production Order** 1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a. a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and b. a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. 2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 3. For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a. the type of communication service used, the technical provisions taken thereto and the period of service;	**No equivalent**	**Legal Analysis** This is an essential provision for an effective cybercrime investigation and its absence will impact upon prosecutions and international cooperation. **Gap Analysis** **Recommendation:** This essential power is necessary to ensure CSPs in Lebanon provide BSI, traffic data and stored content data. This will also require definitions of *"computer data"*, *"subscriber information or BSI"*, *"traffic data"* and *"Communication Service Provider"*.[274] Article 25 CITO is a model that could be used and uses different definitions including *"information technology"*,[275] *"service provider"*[276] and *"data"*[277] – it is still advisable to have definitions for *"subscriber information or BSI"*, *"traffic data"* as they will be different types of evidence that can be produced from CSPs. Further, this power will require individuals and others (such as corporate entities, financial institutions and other organisations) who hold data to produce it to law enforcement authorities. Article 18 BC and section 22 HIPCAR could be a guide with consistent application of definitions

[274] See definitions above

[275] Article 2(1) CITO: "*any material or virtual means or group of interconnected means used to store, sort, arrange, retrieve, process, develop and exchange information according to commands and instructions stored therein. This includes all associated inputs and outputs, by means of wires or wirelessly, in a system or network.*"

[276] Article 2(2) CITO: "*any natural or juridical person, common or private, who provides subscribers with the services needed to communicate through information technology, or who processes or stores information on behalf of the communication service or its users.*"

[277] Article 2(3) CITO: "*all that may be stored, processed, generated and transferred by means of information technology, such as numbers, letters, symbols, etc…*"

Procedure		
International Best Practice	National Legislation	Comments
b. the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c. c.any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement. **Section 22 HIPCAR – Production Order** If a [judge] [magistrate] is satisfied on the basis of an application by a [law enforcement] [police] officer that specified computer data, or a printout or other information, is reasonably required for the purpose of a criminal investigation or criminal proceedings, the [judge] [magistrate] may order that: • a person in the territory of [enacting country] in control of a computer system produce from the system specified computer data or a printout or other intelligible output of that data; or • an Internet service provider in [enacting country] to produce information about persons who subscribe to or otherwise use the service. **Article 25 CITO - Order to Submit Information** Every State Party shall commit itself to adopting the procedures necessary to enable the competent authorities to issue orders to: 1. Any person in its territory to submit certain information in his possession which is stored on information technology or a medium for storing information.		

Procedure		
International Best Practice	**National Legislation**	**Comments**
2. Any service provider offering his services in the territory of the State Party to submit user's information related to that service which is in the possession of the service provider or under his control.		
Article 21 BC **Interception of content data** 1. Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: a. collect or record through the application of technical means on the territory of that Party, and b. compel a service provider, within its existing technical capability: i. to collect or record through the application of technical means on the territory of that Party, or ii. to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system. 2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.	**Law 140/99, amended by the Law 158/99.** **Articles 2, 3 and 9**	**Legal Analysis** Law 140/99, as amended by Law 158/99. allows for interception, listening, and surveillance of all means of communication - including e-mails Interception can only take place after a judicial or an administrative decision has been taken as prescribed by Articles 2 and 3 of Law 140/99 for a maximum period of two months, which is renewable. Article 2 allows for interception in very urgent cases, for offences that are sanctioned for a duration of imprisonment not less than a year. Article 9 allows the Minister of Defence and the Minister of Interior to order interception, after the approval of the Prime Minister to collect information for terrorist and organized crime offences. This power is essential for national legislation – and there must be safeguards and requirement/procedure to compel CSPs cooperation to collect or record content data in real-time of specific communications in Lebanon. **Gap Analysis** **Recommendations:** Provision should be made to compel CSPs in Lebanon (beyond just emails e.g. messaging apps) to cooperate with real-time collection of content; and safeguards should be incorporated to ensure the collection is legal, necessary, reasonable and proportionate in the circumstances. Consideration should be given to reviewing Article 29 of CITO, Article 21 BC and section 26 HIPCAR and incorporating language in national legislation

Procedure		
International Best Practice	**National Legislation**	**Comments**
3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15. **Section 26 HIPCAR – Interception of Content Data** 1. If a [judge] [magistrate] is satisfied on the basis of [information on oath] [affidavit] that there are reasonable grounds to [suspect] [believe] that the content of electronic communications is reasonably required for the purposes of a criminal investigation, the magistrate [may] [shall]: • order an Internet service provider whose service is available in [enacting country] through application of technical means to collect or record or to permit or assist competent authorities with the collection or recording of content data associated with specified communications transmitted by means of a computer system; or • authorize a [law enforcement] [police] officer to collect or record that data through application of technical means. 2. A country may decide not to implement section 26.		

Procedure		
International Best Practice	**National Legislation**	**Comments**
Article 29 CITO - Interception of Content Information 1. Every State Party shall commit itself to adopting the legislative procedures necessary as regards a series of offences set forth in the domestic law, in order to enable the competent authorities to: a. gather or register through technical means in the territory of this State Party, or b. cooperate with and help the competent authorities to expeditiously gather and register content information of the relevant communications in its territory and which are transmitted by means of the information technology. 2. If, because of the domestic legal system, the State Party is unable to adopt the procedures set forth in paragraph 1(a), it may adopt other procedures in the form necessary to ensure the expeditious gathering and registration of content information corresponding to the relevant communications in its territory using the technical means in that territory. 3. Every State Party shall commit itself to adopting the procedures necessary to require the service provider to maintain the secrecy of any information when exercising the authority set forth in this Article.		

Procedure		
International Best Practice	**National Legislation**	**Comments**
Article 20 BC[278] **Real-time collection of traffic data** 1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a. collect or record through the application of technical means on the territory of that Party, and b. compel a service provider, within its existing technical capability: i. to collect or record through the application of technical means on the territory of that Party; or ii. to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.	**No equivalent**	**Legal Analysis** There is no procedural power to collect traffic data real-time. There could be a lower threshold to collect real-time traffic data which is an essential investigative tool. There may be situations where a higher legal threshold to secure content is not made out by an applicant – but a lower threshold to secure traffic could be. For this reason, there should be a distinction between real-time collection of stored content and traffic data. There must be safeguards and requirements/ procedure to compel CSPs cooperation to collect or record content data in real-time of specific communications in Lebanon **Gap Analysis** **Recommendations:** There should be a specific power to collect traffic data real-time and provision should be made to compel CSPs in Lebanon to cooperate with real-time collection of traffic data; and safeguards should be incorporated to ensure the collection is legal, necessary, reasonable and proportionate in the circumstances. The language from Article 28 CITO could be considered but this does not refer to real-time only expeditious collection. Article 20 BC and section 25 HIPCAR should be used as a guide for national legislation

[278] Article 28 CITO refers to expeditious collection rather than real-time collection

Procedure		
International Best Practice	National Legislation	Comments
3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15. **Section 25 HIPCAR - Collection of Traffic Data** 1. If a [judge] [magistrate] is satisfied on the basis of [information on oath][affidavit] that there are reasonable grounds to [suspect] [believe] that traffic data associated with a specified communication is reasonably required for the purposes of a criminal investigation, the [judge] [magistrate] [may] [shall] order a person in control of such data to: • collect or record traffic data associated with a specified communication during a specified period; or • permit and assist a specified [law enforcement] [police] officer to collect or record that data. 2. If a [judge] [magistrate] is satisfied on the basis of [information on oath] [affidavit] that there are reasonable grounds to [suspect] [believe] that traffic data is reasonably required for the purposes of a criminal investigation, the [judge] [magistrate] [may] [shall] authorize a [law enforcement] [police] officer to collect or record traffic data associated with a specified communication during a specified period through application of technical means.		

Procedure

International Best Practice	National Legislation	Comments
3. A country may decide not to implement section 25.		
		Disclosure obligation of encryption keys With terrorists and organized criminals routinely using encrypted messaging applications[279] this may be considered a viable power to release the keys to passwords to unlock devices[280] **Gap Analysis** **Recommendation:** Unable to clarify if there were any such powers in Lebanon – but such a power will allow law enforcement to compel owners to unlock devices
		Data retention obligations[281] Such a power can allow law enforcement to 1. Trace and identify the source of a communication 2. Identify the destination of a communication; 3. Identify the date, time and duration of a communication; and 4. Identify the type of communication Lebanon does have such an obligation[282]

International Cooperation

International Best Practice	National Legislation	Comments
Article 22 BC **Jurisdiction** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:	**No equivalent**	**Legal Analysis** Without a clearly defined scope for cybercrime offences, that are international in nature, any legislation will be restricted. **Gap Analysis** **Recommendation:** National legislation ensures jurisdiction is defined using the language of Article 22 BC, section 19 HIPCAR or Article 30 CITO.

[279] Eleanor Saitta. "Can Encryption Save Us?" Nation 300, no. 24 (June 15, 2015): 16-18. Academic Search Premier, EBSCOhost (accessed February 29, 2016).

[280] For an example see section 49 Regulation of Investigatory Powers Act 2000 (UK) - http://www.legislation.gov.uk/ukpga/2000/23/section/49

[281] In 2006 the EU issued its Data Retention Directive - EU Member States had to store electronic telecommunications data for at least six months and at most 24 months for investigating, detecting and prosecuting serious crime. In 2014, the Court of Justice of the EU invalidated the Data Retention Directive, holding that it provided insufficient safeguards against interferences with the rights to privacy and data protection. In the absence of a valid EU Data Retention Directive, Member States may still provide for a data retention scheme – for national schemes see: http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention

[282] ICMEC Global Review page 30

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
a. in its territory; or b. on board a ship flying the flag of that Party; or c. on board an aircraft registered under the laws of that Party; or d. by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. 2. Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 3. Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition. 4. This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. 5. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.		If there is a conflict between jurisdictions consideration should be given to guidelines on determining the appropriate jurisdiction to try an offence – see the Eurojust Guidelines for Deciding which Jurisdiction should Prosecute (revised 2016)[283]

[283] http://www.eurojust.europa.eu/Practitioners/operational/Documents/Operational-Guidelines-for-Deciding.pdf

International Cooperation		
International Best Practice	National Legislation	Comments
Section 19 HIPCAR – Jurisdiction This Act applies to an act done or an omission made: • in the territory of [enacting country]; or • on a ship or aircraft registered in [enacting country]; or • by a national of [enacting country] outside the jurisdiction of any country; or by a national of [enacting country] outside the territory of [enacting country], if the person's conduct would also constitute an offence under a law of the country where the offence was committed. **Article 30 CITO - Competence** 1. Every State Party shall commit itself to adopting the procedures necessary to extend its competence to any of the offences set forth in Chapter II of this Convention, if the offence is committed, partly or totally, or was realized: a. in the territory of the State Party b. on board a ship raising the flag of the State Party. c. on board a plane registered under the law of the State Party. d. by a national of the State Party if the offence is punishable according to the domestic law in the location where it was committed, or if it was committed outside the jurisdiction of any State. e. if the offence affects an overriding interest of the State.		

International Cooperation		
International Best Practice	National Legislation	Comments
2. Every State Party shall commit itself to adopting the procedures necessary to extend the competence covering the offences set forth in Article 31, paragraph 1, of this Convention in the cases in which the alleged offender is present in the territory of that State Party and shall not extradite him to another Party according to his nationality following the extradition request. 3. If more than one State Party claim to have jurisdiction over an offence set forth in this Convention, priority shall be accorded to the request of the State whose security or interests were disrupted by the offence, followed by the State in whose territory the offence was committed, and then by the State of which the wanted person is a national. In case of similar circumstances, priority shall be accorded to the first State that requests the extradition.		

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
Article 35 BC[284] **24/7 Network** 1. Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures: a. the provision of technical advice; b. the preservation of data pursuant to Articles 29 and 30; c. the collection of evidence, the provision of legal information, and locating of suspects. 2. a. A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis. b. If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to coordinate with such authority or authorities on an expedited basis. 3. Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.	**No equivalent**	**Legal Analysis** This is an essential mechanism for an effective cybercrime investigative capability. **Gap Analysis** **Recommendation:** This should not require legislation to implement and subject to resources should be established as a priority. Contact details should be shared for the nominated single point of contact (SPOC) nationally, central authorities internationally and INTERPOL. Consideration should also be given to drafting a Memorandum of Understanding with national agencies so that the SPOC has authority to undertake the actions required as part of an international cybercrime investigation applying national laws and treaties.This MOU will include both incoming and outgoing requests and ensure an efficient and effective process.

[284] Article 43 CITO

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
Article 25 BC **General principles relating to mutual assistance** 1. The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. 2. Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35. 3. Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.	**No equivalent**	**Legal Analysis** Lebanon is not a party to the BC or CITO. Lebanon is not a party to an international convention dedicated to cybercrime, this will hinder international investigations as procedural powers will not have a legal basis. Other than any bilateral treaty – Lebanon is a signatory to UNTOC[285] so Article 18 UNTOC is the basis for MLA and mutuality/ reciprocity.[286] This means that without national legislation requests cannot be made for expedited preservation of stored computer data, expedited preservation and partial disclosure of traffic data and disclosure of stored data and traffic data, meaning a limitation to the international cooperation that Lebanon can provide to Requesting States. **Gap Analysis** **Recommendation:** Domestic law is required for expedited preservation of stored computer data, expedited preservation and partial disclosure of traffic data and production orders. The BC, HIPCAR and CITO can be used as precedents for expedited preservation of stored computer data,[287] expedited preservation and partial disclosure of traffic data[288] disclosure of stored data[289] and expedited gathering of traffic data[290] - there also needs to be consideration of provision for real-time interception of traffic data and content[291]. Further, there needs to be a framework to cooperate on cybercrime investigations provided by multilateral conventions such as Article 27 BC and Article 32 CITO.[292]

[285] Ratified 5 October 2005

[286] UNTOC Article 18 could be the basis for MLA if definition of transnational organized crime satisfied and also Riyadh Agreement on Judicial Cooperation could be a basis to States who have ratified

[287] Article 29 BC, section 23 HIPCAR and Article 37 CITO

[288] Article 30 BC, sections 23 and 24 HIPCAR and Article 38 CITO

[289] Article 31 BC and Article 39 CITO

[290] Article 41 CITO

[291] Article 33 and 34 BC and sections 25 and 26 HIPCAR

[292] There are no equivalent provisions on the procedure for MLA in AUC

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
4. Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation.The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence. 5. Where, in accordance with the provisions of this chapter, the requested Party is permitted to *make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.* **Article 34 CITO - Procedures for Cooperation and Mutual Assistance Requests** 1. The provisions of paragraphs 2-9 of this Article shall apply in case no cooperation and mutual assistance treaty or convention exists on the basis of the applicable legislation between the State Parties requesting assistance and those from which assistance is requested. If such a treaty or convention exists, the mentioned paragraphs shall not apply, unless the concerned parties agree to apply them in full or in part.		Consideration should be given to allowing adjudicating authorities to authorise domestic law enforcement to investigate in the State where access to a device is known. Accessibility of information is the essential criterion to initiate an investigation in cases where it is not possible to know where the data is stored (i.e. in the cloud). This could include a *"mutual recognition"* of court orders issued towards communication service providers in a given State, that could be served to branches of that CSPs located in *other States, depending on where the data is stored.*

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
2. a. Every State Party shall designate a central authority responsible for sending and responding to mutual assistance requests and for their implementation and referral to the relevant authorities for implementation. b. Central authorities shall communicate directly among themselves. c. Every State Party shall, at the time of signature or deposit of the instrument of ratification, acceptance or agreement, contact the General Secretariat of the Council of Arab Interior Ministers and the Technical Secretariat of the Arab Justice Ministers and communicate to them the names and addresses of the authorities specifically designated for the purposes of this paragraph. d. The General Secretariat of the Council of Arab Interior Ministers and the Technical Secretariat of the Arab Justice Ministers shall establish and update a registry of concerned central authorities appointed by the State Parties. Every State Party shall insure that the registry's details are correct at all times 3. Mutual assistance requests in this Article shall be implemented according to procedures specified by the requesting State Party, except in the case of non conformity with the law of the State Party from which assistance is requested.		

International Cooperation		
International Best Practice	National Legislation	Comments
4. The State Party from which assistance is requested may postpone taking action on the request if such action shall affect criminal investigations conducted by its authorities. 5. Prior to refusing or postponing assistance, the State Party from which assistance is requested shall decide, after consulting with the requesting State Party, whether the request shall be partially fulfilled or be subject to whatever conditions it may deem necessary. 6. The State Party from which assistance is requested shall commit itself to inform the requesting State Party of the result of the implementation of the request. If the request is refused or postponed, the reasons of such refusal or postponement shall be given. The State Party from which assistance is requested shall inform the requesting State Party of the reasons that prevent the complete fulfilment of the request or the reasons for its considerable postponement. 7. The State Party requesting assistance may request the State Party from which assistance is requested to maintain the confidentiality of the nature and content of any request covered by this chapter, except in as far as necessary to implement the request. If the State Party from which assistance is requested cannot abide by this request concerning confidentiality, it shall so inform the requesting State Party which will then decide about the possibility of implementing the request.		

International Cooperation		
International Best Practice	National Legislation	Comments
8. a. In case of emergency, mutual assistance requests may be sent directly to the judicial authorities in the State Party from which assistance is requested from their counterparts in the requesting State Party. In such case, a copy shall be sent concurrently from the central authority in the requesting State Party to its counterpart in the State Party from which assistance is requested. b. Communications can be made and requests submitted pursuant to this paragraph through INTERPOL. c. Whenever, according to paragraph a, a request is submitted to an authority, but that authority is not competent to deal with that request, it shall refer the request to the competent authority and directly inform the requesting State Party accordingly. d. Communications and requests carried out according to this paragraph and not concerning compulsory procedures may be transmitted directly by the competent authorities in the requesting State Party to their counterpart in the State Party from which assistance is requested.		

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
e. Every State Party may, at the time of signature, ratification, acceptance or adoption, inform the General Secretariat of the Council of Arab Interior Ministers and the Technical Secretariat of the Arab Justice Ministers that requests according to this paragraph must be submitted to the central authority for reasons of efficiency.		
Article 26 BC **Spontaneous Information** 1. A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter. 2. Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.		**Legal Analysis** This is an important procedure to enable a state privy to information that will assist another state to prevent a cybercrime or to investigate it. Albeit available between CITO ratified states in CITO Article 33, Lebanon has no domestic legal basis to share such information with non-CITO states unless an official request is sent through the usual MLA channels. Article 18(4)-(5) UNTOC provides for the sharing of intelligence spontaneously for matters fulfilling the definition of a serious crime293, that is transnational[294] and involves an organized crime group[295]. Without satisfying this definition an official request will need to be sent through the usual MLA channels to non-CITO states. On the basis of the fast-moving nature of cybercriminality spontaneous sharing is an effective way to cooperate with other states and its absence inhibits effective international collaboration with non-CITO states.

[293] Article 2(b) UNTOC "*"Serious crime" shall mean conduct constituting an offence punish- able by a maximum deprivation of liberty of at least four years or a more serious penalty*"

[294] Article 3(1) UNTOC

[295] Article 2(a) UNTOC "*"Organized criminal group" shall mean a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit*"

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
Article 33 CITO - Circumstantial Information 1. A State Party may – within the confines of its domestic law – and without prior request, give another State information it obtained through its investigations if it considers that the disclosure of such information could help the receiving State Party in investigating offences set forth in this convention or could lead to a request for cooperation from that State Party. 2. Before giving such information, the State Party providing it may request that the confidentiality of the information be kept; if the receiving State Party cannot abide by this request, it shall so inform the State Party providing the information which will then decide about the possibility of providing the information. If the receiving State Party accepts the information on condition of confidentiality, the information shall remain between the two sides.	**No equivalent**	**Gap Analysis** **Recommendation:** Use UNTOC Article 18(4)-(5) as the basis to spontaneously share information that fulfils the scope of UNTOC (with guarantees provided about use in evidence or disclosure of sensitive information to a third party (including another state).[296] Consider legislation based on Article 33 CITO or Article 26 BC.
Article 32 BC **Trans-border access to stored computer data with consent or where publicly available** A Party may, without the authorisation of another Party: a. access publicly available (open source) stored computer data, regardless of where the data is located geographically; or b. access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.	**No equivalent**	**Legal Analysis** This procedural power enables a state to secure content stored in another state in limited circumstances. Article 32.b. BC and Article 40 CITO is an exception to the principle of territoriality and permits unilateral trans-border access without the need for mutual legal assistance where there is consent or the information is publicly available. Examples of use of this procedural power under BC Article 32.b. include: A person's e-mail may be stored in another country by a service provider, or a person may intentionally store data in another country. These persons may retrieve the data and, provided that they have the lawful authority, they may voluntarily disclose the data to law enforcement officials or permit such officials to access the data[297]

[296] See Article 33(2) CITO

[297] Paragraph 294 page 53 BC Explanatory Report

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
Section 27 HIPCAR – Forensic Software 1. If a [judge] [magistrate] is satisfied on the basis of [information on oath] [affidavit] that in an investigation concerning an offence listed in paragraph 7 herein below there are reasonable grounds to believe that essential evidence cannot be collected by applying other instruments listed in Part IV but is reasonably required for the purposes of a criminal investigation, the [judge] [magistrate] [may] [shall] on application authorize a [law enforcement] [police] officer to utilize a remote forensic software with the specific task required for the investigation and install it on the suspect's computer system in order to collect the relevant evidence. The application needs to contain the following information: • suspect of the offence, if possible with name and address; and • description of the targeted computer system; and • description of the intended measure, extent and duration of the utilization; • reasons for the necessity of the utilization.		A suspected terrorist is lawfully arrested while his/her mailbox – possibly with evidence of a crime – is open on his/her tablet, smartphone or other device. If the suspect voluntarily consents that the police access the account and if the police are sure that the data of the mailbox is located in another state, police may access the data under Article 32.b. **Gap Analysis** **Recommendation:** This restricted power to unilaterally secure evidence is included in legislation with safeguards to ensure the consent is lawfully obtained from the user.[298] Language can be used from Article 32 BC and Article 40 CITO. Article 32.b. has been heavily criticized and it may be considered that the consent of the state where the stored computer data is stored is obtained in addition to the user. Section 27 HIPCAR provides for forensic software and this may allow access to a computer in another state. There are a number of restrictions that requires the evidence cannot be obtained by other means, a judicial order is required, can only apply to certain offences and is for a restricted period (3 months). Consideration should also be given to consent of the other state where the forensic software may intrude.

[298] Consideration should be given to situations such as the non-availability of a user (e.g. death) and if consent can be obtained in another state

International Cooperation		
International Best Practice	National Legislation	Comments
2. Within such investigation it is necessary to ensure that modifications to the computer system of the suspect are limited to those essential for the investigation and that any changes if possible can be undone after the end of the investigation. During the investigation, it is necessary to log: - the technical mean used and time and date of the application; and • the identification of the computer system and details of the modifications undertaken within the investigation; • any information obtained. Information obtained by the use of such software needs to be protected against any modification, unauthorized deletion and unauthorized access. 3. The duration of authorization in section 27 (1) is limited to [3 months]. If the conditions of the authorization is no longer met, the action taken are to stop immediately. 4. The authorization to install the software includes remotely accessing the suspects computer system. 5. If the installation process requires physical access to a place the requirements of section 20 need to be fulfilled. 6. If necessary a [law enforcement] [police] officer may pursuant to the order of court granted in (1) above request that the court order an internet service provider to support the installation process. 7. [List of offences]. 8. A country may decide not to implement section 27.		

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
Article 40 CITO - Access to Information Technology Information Across Borders A State Party may, without obtaining an authorization from another State Party: 1. Access information technology information available to the public (open source), regardless of the geographical location of the information. 2. Access or receive – through information technology in its territory – information technology information found in the other State Party, provided it has obtained the voluntary and legal agreement of the person having the legal authority to disclose information to that State Party by means of the said information technology.		

Morocco[299]

Signed and ratified the BC in 2012

Offences		
International Best Practice	**National Legislation**	**Comments**
Article 2 BC – Illegal access[300] Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system. **Article 6 CITO – Illicit Access** 1. Illicit access to, presence in or contact with part or all of the information technology, or the perpetuation thereof. 2. The punishment shall be increased if this access, presence, contact or perpetuation leads to: a. the obliteration, modification, distortion, duplication, removal or destruction of saved data, electronic instruments and systems and communication networks, and damages to the users and beneficiaries. b. the acquirement of secret government information.	**Penal Code** **Article 607-3** Fraudulent access to all or part of an automated data processing system …. Anyone who maintains himself or herself in all or part of an automated data processing system to which he has accessed in error and who is not entitled to it is liable to the same penalty. The penalty shall be doubled if it has resulted either in the deletion or modification of data contained in the automated data processing system or in an alteration in the operation of the system. **Article 607-4** Without prejudice to more severe penal provisions, a person who commits the acts provided for in the preceding article shall be punished from six months to two years of imprisonment and from 10,000 to 100,000 dirhams of fine for all or part of an automated data processing system supposed to contain information relating to the internal or external security of the State or the secrets concerning the national economy.	**Legal Analysis** The national provision includes reference to *"fraudulently"* this would suggest that the perpetrator has accessed the data dishonestly – whereas the BC refers to *"without right"* on the basis access is unauthorized. The BC refers to a "dishonest intent" but this is the mens rea to secure data rather than the act of gaining illegal access. At present this national offence can only be committed where the perpetrator dishonestly represents the purpose for accessing. It is unclear without a definition of *"fraudulently"* if this requires an overt action or if every illegal access is deemed to be fraudulent. It is for this reason that a definition of *"fraudulent"* is required. CITO refers to *"illicit access to, presence in or contact with"* without defining what these acts mean – therefore, BC and HIPCAR are to be preferred. The offence also refers to a *"automated data processing system"* without a definition. It is unclear if this relates to a *"computer system"* (i.e. means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data – Article 1 BC) or *"computerised data"* (i.e. any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function – Article 1 BC) The aggravated form of the offence in Article 607-4 could be wider to include all national interests of the State such as health.

[299] A draft bill on the Code of Criminal Procedure will be presented soon to the Moroccan Parliament for ratification; it includes the elements presented in this report in the form of recommendations.

[300] Article 29(1) AUC

Offences		
International Best Practice	**National Legislation**	**Comments**
Section 4 HIPCAR – Illegal Access 1. A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, accesses the whole or any part of a computer system commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. 2. A country may decide not to criminalize the mere unauthorized access provided that other effective remedies are available. Furthermore, a country may require that the offence be committed by infringing security measures or with the intent of obtaining computer data or other dishonest intent. **Section 5 HIPCAR – Illegal Remaining** 1. A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, remains logged in a computer system or part of a computer system or continues to use a computer system commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. 2. A country may decide not to criminalize the mere unauthorized remaining provided that other effective remedies are available. Alternatively, a country may require that the offence be committed by infringing security measures or with the intent of obtaining computer data or other dishonest intent.		**Gap Analysis** **Recommendation:** The national legislation could incorporate relevant language from the BC and HIPCAR to include definitions of a computer system[301] and the inclusion of programs within the definition of data as some data includes programs and other data does not. Further, to be consistent with the BC and HIPCAR refer to access *"without right"* rather than fraudulently. The aggravated offence in Article 607-4 could be wider to take into account illegal access to critical infrastructure data, rather than just that *related to national security and the economy see section 4(2) HIPCAR*

[301] See Article 1.a. BC: "*any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data*" **or** section 3(5) HIPCAR: "*a device or a group of inter-connected or related devices, including the Internet, one or more of which, pursuant to a program, performs automatic processing of data or any other function*"

Offences		
International Best Practice	**National Legislation**	**Comments**
Article 3 BC[302] **Illegal Interception** Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system. **Article 7 CITO** **Illicit Interception** The deliberate unlawful interception of the movement of data by any technical means, and the disruption of transmission or reception of information technology data. **Section 6 HIPCAR – Illegal Interception** 1. A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, intercepts by technical means: • any non-public transmission to, from or within a computer system; or • electromagnetic emissions from a computer system commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.	**No equivalent**	**Legal Analysis** This offence is essential to prosecute non-public transmissions of computer data to, from, or within a computer system that may be illegally intercepted to obtain information about a person's location (e.g. to target that person).[303] ID theft often entails the use of keyloggers or other types of malware for the illegal interception of non-public transmissions of computer data to, from or within a computer system containing sensitive information such as identity information. This offence is essential to prosecute transmissions of computer data to, from, or within a computer system that may be illegally intercepted to obtain information (e.g. wikileaks or Panama Papers). The language in Article 7 CITO (illegal interception) has no definition of *"information technology data"* **Gap Analysis** **Recommendation:** Article 7 CITO with a definition of *"information technology data"* or Article 3 BC or section 6 HIPCAR can be used as a guide for national legislation

[302] Article 29(2) AUC

[303] http://www.coe.int/en/web/cybercrime/guidance-notes

Offences		
International Best Practice	**National Legislation**	**Comments**
2. A country may require that the offence be committed with a dishonest intent, or in relation to a computer system that is connected to another computer system, or by circumventing protection measures implemented to prevent access to the content of non-public transmission.		
Article 4 BC[304] **Data Interference** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm. **Section 7 HIPCAR – Illegal Data Interference** A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, does any of the following acts: • damages or deteriorates computer data; or • deletes computer data ; or • alters computer data; or • renders computer data meaningless, useless or ineffective; or • obstructs, interrupts or interferes with the lawful use of computer data; or • obstructs, interrupts or interferes with any person in the lawful use of computer data; or	**Penal Code** **Article 607-6** The fraudulent introduction of data into an automated data processing system or the fraudulent deterioration or deletion of data contained therein, the way in which it is processed or transmitted	**Legal Analysis** The use of "fraudulently" is inconsistent (in fact in conflict with) the standard of the BC 4.1 "…when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right" which does not require fraud to be proved. This basically means that conduct which constitutes an offence of data interference under the BC's 4.1 would not be criminalized under Article 607-6 This Article does not include element of suppression of computer data **Gap Analysis** **Recommendation:** Use Article 4 BC or section 7 HIPCAR as a guide for national legislation

[304] Article 29(1)(e-f) AUC

Offences		
International Best Practice	**National Legislation**	**Comments**
• denies access to computer data to any person authorized to access it; commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. **Article 8 CITO** **Offence Against the Integrity of Data** 1. Deliberate unlawful destruction, obliteration, obstruction, modification or concealment of information technology data. 2. The Party may require that, in order to criminalize acts mentioned in paragraph 1, they must cause severe damage.		
Article 5 BC[305] **System Interference** Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data. **Section 9 HIPCAR – Illegal System Interference** 1. A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification: • hinders or interferes with the functioning of a computer system; or • hinders or interferes with a person who is lawfully using or operating a computer system;	**Penal Code** **Article 607-5** The intentional hindrance or distortion of the operation of an automated data processing system	**Legal Analysis** This offence would prevent malware that interferes with the functioning of a computer – for example computer worms - a subgroup of malware (like computer viruses). They are self-replicating computer programs that harm the network by initiating multiple data-transfer processes. They can influence computer systems by hindering the smooth running of the computer system, using system resources to replicate themselves over the Internet or generating network traffic that can close down availability of certain services (such as websites) Article 607-5 does not refer to the *"intentional hindrance or distortion"* being *"without right"* Further, Article 607-5 does not refer to the acts of intentional hindrance or distortion by "inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data" Referencing these acts will ensure that the offence describes what intentional hindrance or distortion means.

[305] Article 29(1)(d) AUC no equivalent in CITO

Offences

International Best Practice	National Legislation	Comments
commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. 2. A person who intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification hinders or interferes with a computer system that is exclusively for the use of critical infrastructure operations, or in the case in which such is not exclusively for the use of critical infrastructure operations, but it is used in critical infrastructure operations and such conduct affects that use or impacts the operations of critical infrastructure the punishment shall be imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.		**Gap Analysis** **Recommendation:** Use the BC language in Article 5 by adding *“intentional hindrance or distortion” **without right**” and the acts of inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data”* Also consider whether the prevention and prosecution of attacks against critical infrastructure needs a separate or aggravated offence for example the functioning of a computer system may be hindered for terrorist purposes (e.g. hindering the system that stores stock exchange records can make them inaccurate, or hindering the functioning of critical infrastructure.[306] See precedent at section 9(2) HIPCAR.
Article 6 BC[307] **Misuse of Devices** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a. the production, sale, procurement for use, import, distribution or otherwise making available of: i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;	**Penal Code** **Article 607-10** Is punished with imprisonment of two to five years and a fine from 50,000 to 2,000,000 dirhams for any person to manufacture, acquire, hold, transfer, offer or otherwise disposal of equipment, instruments, computer programs or any data, designed or specially adapted for the offenses provided for in this Chapter.	**Legal Analysis** This offence will enable prosecution for the production, sale, procurement for use, import, distribution of access codes and other computerized data used to commit cybercrimes. - for example, computer systems may be accessed to facilitate a terrorist attack by interfering with a country's electrical power grid. As above for Illicit Access there is no reference to *“without right”* or an intention – an intention to commit the offence would be consistent with the suggested amendments to the preceding offences and also where intention is already stipulated in Article 607-5 Article 607-10 does not specifically criminalise the acts of *“sale, procurement for use, import, or distribution” - albeit there is a catchall of otherwise dispose.*

[306] http://www.coe.int/en/web/cybercrime/guidance-notes

[307] Article 9 CITO and Article 29(1)(h) AUC

Offences		
International Best Practice	National Legislation	Comments
ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b. the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3. Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.		

Offences		
International Best Practice	**National Legislation**	**Comments**
Section 10 HIPCAR – Illegal Devices 1. A person commits an offence if the person: a. intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, produces, sells, procures for use, imports, exports, distributes or otherwise makes available: i. a device, including a computer program, that is designed or adapted for the purpose of committing an offence defined by other provisions of Part II of this law; or ii. a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed; with the intent that it be used by any person for the purpose of committing an offence defined by other provisions of Part II of this law; or b. has an item mentioned in subparagraph (i) or (ii) in his or her possession with the intent that it be used by any person for the purpose of committing an offence defined by other provisions of part II of this law commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.		There is no reference to a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any cybercrime offence. This inclusion would ensure that this criminal behaviour is clearly specified. The BC at Article 6.2. provides for a reasonable excuse if the intentional act is *“for the authorised testing or protection of a computer system.”* This will ensure that law enforcement will not be liable for this offence (also see section 10(2) HIPCAR) Please note that HIPCAR provides the option of listing the devices in a schedule if deemed appropriate – this could be restrictive and require updating with technological progress. **Gap Analysis** **Recommendation:** Use the HIPCAR language at section 10 or BC language in Article 6 by adding *“**without right**”* and an intention to commit this offence – also consideration should be given to specifying the use of passwords and access codes. The Article should provide a reasonable excuse so law enforcement can use devices for special *investigation techniques – the language at Article 6.2. can be used as a guide.*

Offences		
International Best Practice	**National Legislation**	**Comments**
2. This provision shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph I is not for the purpose of committing an offence established in accordance with other provisions of Part II of this law, such as for the authorized testing or protection of a computer system. 3. A country may decide not to criminalize illegal devices or limit the criminalization to devices listed in a Schedule.		
Article 7 BC **Computer related forgery** Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.	**Penal Code** **Article 607-7** Without prejudice to more severe penal provisions, the forgery or falsification of computerized documents, whatever their form, harm to another person,	**Legal Analysis** As above for Illicit Access there is no reference to *"without right"* or an intention – an intention to commit the offence would be consistent with the suggested amendments to the preceding offences and also where intention is already stipulated in Article 607-5 There is no definition of *"computerized documents"* Article 607-7 requires harm whereas the approach of Article 7 is to intend without authorization to input, alteration, deletion, or suppress computer data with fake data, intending that it is acted upon as if real data. There is no requirement that harm or loss is actually caused to another. This added requirement by Article 607-7 may restrict the number of successful prosecutions as there maybe occasions when no harm is caused by the intent to do so was clearly present. For example, in a spear phishing scam, a forged back statement with a inauthentic URL is distributed, but the user does not act upon it, causing no harm.

Offences		
International Best Practice	**National Legislation**	**Comments**
Section 11 HIPCAR – Computer-related Forgery 1. A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification inputs, alters, deletes, or suppresses computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. 2. If the abovementioned offence is committed by sending out multiple electronic mail messages from or through computer systems, the penalty shall be imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. **Article 10 CITO** **Offence of Forgery** The use of information technology means to alter the truth of data in a manner that causes harm, with the intent of using them as true data. **Article 29(2)(b) AUC** Intentionally input, alter, delete, or suppress computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable and intelligible. A Party may require intent to defraud, of similar dishonest intent, before criminal liability attaches		**Gap Analysis** **Recommendation:** A definition is provided of *"computerized documents"* and consideration given to replacing with *"computer data"* as defined in Article 1.b. BC Inclusion of *"without right"* and an intention to commit the offence – consideration should be given as to whether this is a dishonest intent. A review as to whether harm needs to be an element of the offence – it is preferable not to use harm so that the forgery is committed as soon as the inauthentic data is created and considered. This would mean if a forged link or document is sent as part of a phishing scam the offence is complete as soon as the recipient considers it (i.e. opens the email containing the link or opens the attached document) – rather than having to prove the recipient has suffered any harm

Offences		
International Best Practice	**National Legislation**	**Comments**
Article 8 BC[308] **Computer related fraud** Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a. any input, alteration, deletion or suppression of computer data, b. any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person. **Section 12 HIPCAR – Computer-related Fraud** A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification causes a loss of property to another person by: • any input, alteration, deletion or suppression of computer data; • any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person the penalty shall be imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.	**Penal Code** **Article 607-6** The fraudulent introduction of data into an automated data processing system or the fraudulent deterioration or deletion of data contained therein, the way in which it is processed or transmitted, is punishable by one to three years imprisonment and from 10,000 to 200,000 dirhams of fines or of either of these penalties alone **Dahir No. 1-09-15 of 22 safar 1430 (18 February 2009) promulgating Law No. 09-08 on the protection of individuals with regard to the processing of personal data** **Article 54** Anyone who, contrary to (a), (b) and (c) of the present Convention, is punishable by imprisonment from three months to one year and a fine of 20,000 to 200,000 DH Article 3 of this Law, the collection of personal data by fraudulent, unfair or illicit means, performs treatment for purposes other than those declared or authorized or subjects the above data to further processing incompatible with the purposes declared or authorized.	**Legal Analysis** Whilst *"fraudulently'* in this context does provide a certain degree of protection, the absence of the actus reus of committing this conduct without authorization is missing and may create uncertainty. There is no definition of *"data"* or *"automated data processing system"* and may create uncertainty. Articles 54 and 61 can criminalise the dissemination of personal data. These articles would not criminalise the negligent breach of personal data, such as misplacing data or inadvertently sent to an incorrect addressee. Albeit section 61 does refer to negligence, the data disclosed would have to be put to a fraudulent purpose to prove the offence. **Gap Analysis** **Recommendation:** Providing definitions for *"data"* and *"automated data processing system"* and including *"without right"* in Article 607-6. The language in BC or HIPCAR for this offence is a good guide for national legislation

[308] Article 11 CITO and Article 29(2)(d) AUC

Offences		
International Best Practice	**National Legislation**	**Comments**
	Article 61 A prisoner shall be punished with imprisonment from six months to one year and with a fine of between 20,000 and 300,000 DH, or one of these two penalties only, any person responsible for treatment, any subcontractor and any person who, By reason of his / her duties, is responsible for processing personal data and who, even through negligence, causes or facilitates the abuse or fraudulent use of the data processed or received or communicates them to unauthorized third parties. The court may also order the seizure of the material used to commit the offense and the deletion of all or part of the personal data subject to the processing which gave rise to the infringement.	
Article 9 BC[309] **Content related offences (e.g. child pornography)** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a. producing child pornography for the purpose of its distribution through a computer system; b. offering or making available child pornography through a computer system; c. distributing or transmitting child pornography through a computer system;	**Penal Code** **Article 503 - 2** Anyone who causes, incites or facilitates the exploitation of children under the age of eighteen years in pornography by any representation, by any means whatsoever, of any actual, simulated or perceived sexual act or any representation of the sexual organs of A child for purposes of a sexual nature….. The same penalty applies to anyone who produces, disseminates, publishes, imports, exports, exhibits, sells or holds similar pornographic materials. These acts are punished even if their elements are committed outside the Kingdom.	**Legal Analysis** This is an essential offence in order to protect children from harm by criminalizing the distribution, transmitting, making available, offering, producing and possession of indecent images of children. Article 503-2 does not specifically refer to any of the acts of *"produces, disseminates, publishes, imports, exports, exhibits, sells"* being through a computer system or network or storage medium. Whilst protection is provided by the extra-territoriality reference, stipulating use of a computer system will provide specificity for any element committed either in or outside of the Kingdom. Article 9.1. also refers to the following acts which are not included in Article 503-2 *"offering or making available child pornography through a computer system", procuring child pornography through a computer system for oneself or for another person",*

[309] Article 12 CITO and Article 29(3)(a-d) AUC

Offences		
International Best Practice	**National Legislation**	**Comments**
d. procuring child pornography through a computer system for oneself or for another person; e. possessing child pornography in a computer system or on a computer-data storage medium. 2. For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: a. a minor engaged in sexually explicit conduct; b. a person appearing to be a minor engaged in sexually explicit conduct; c. realistic images representing a minor engaged in sexually explicit conduct. 3. For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years. 4. Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c. **Section 13 HIPCAR – Child Pornography** 1. A person who, intentionally, without lawful excuse or justification: • produces child pornography for the purpose of its distribution through a computer system; • offers or makes available child pornography through a computer system; • distributes or transmits child pornography through a computer system;		**Gap Analysis** **Recommendation:** The acts under Article 503-2 are extended to include *"offering or making available child pornography through a computer system"*, procuring child pornography through a computer system for oneself or for another person", (see Article 9.1.b BC) Article 503-2 specifically refers to the acts being carried out through a computer system, network or storage device – see section 13 HIPCAR

Offences		
International Best Practice	**National Legislation**	**Comments**
- procures and/or obtain child pornography through a computer system for oneself or for another person; - Possesses child pornography in a computer system or on a computer- data storage medium; or - knowingly obtains access, through information and communication technologies, to child pornography, commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. 2. It is a defense to a charge of an offence under paragraph (1) (b) to (1)(f) if the person establishes that the child pornography was a bona fide law enforcement purpose. 3. A country may not criminalize the conduct described in section 13 (1)(d)- (f).		
Article 10 BC[310] **Infringement of copyright**	**Dahir No. 1-00-20 of 9 kaada 1420 (15 February 2000) promulgating Law No. 2-00 on Copyright and Neighboring Rights** **Article 64**	This is adequately drafted

[310] Article 17 CITO and no equivalent in AUC

Offences		
International Best Practice	National Legislation	Comments
Article 11 BC[311] **Aiding and Abetting** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed. 2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention. **Article 19 CITO - Attempt at and Participation in the Commission of Offences** 1. Participation in the commission of any of the offences set forth in this chapter with the intention to commit the offence in the law of the State Party. 2. Attempt at the commission the offences set forth in Chapter II of this convention. 3. A State Party may reserve the right to not implement the second paragraph of this Article totally or partly.	**Criminal Code** **Articles 114 and 129**	**Legal Analysis** Aiding and abetting others to commit offences is essential in order to prosecute those who may have provided assistance or encouraged cybercrimes to take place. **In case of aiding and abetting in cybercrime, the general rules contained in the Criminal Code Articles 129 apply.** **Article 114 provides for attempts to commit criminal offences.**

[311] Article 29(2)(f) AUC

Offences		
International Best Practice	**National Legislation**	**Comments**
Article 12 BC[312] **Corporate liability** 1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on: a. a power of representation of the legal person; b. an authority to take decisions on behalf of the legal person; c. an authority to exercise control within the legal person. 2. In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority. 3. Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative. 4. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.	**No equivalent**	**Legal Analysis** This provision is an essential element so that legal persons (e.g. corporate entities) acting on behalf of natural persons have criminal liability **Gap Analysis** **Recommendation:** Use the BC language in Article 12 as a guide for national legislation

[312] Article 20 CITO and Article 30(2) AUC

Offences		
International Best Practice	**National Legislation**	**Comments**
Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems **Article 3[313] – Dissemination of racist and xenophobic material through computer systems** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: distributing, or otherwise making available, racist and xenophobic material to the public through a computer system. 2. A Party may reserve the right not to attach criminal liability to conduct as defined by paragraph 1 of this article, where the material, as defined in Article 2, paragraph 1, advocates, promotes or incites discrimination that is not associated with hatred or violence, provided that other effective remedies are available. 3. Notwithstanding paragraph 2 of this article, a Party may reserve the right not to apply paragraph 1 to those cases of discrimination for which, due to established principles in its national legal system concerning freedom of expression, it cannot provide for effective remedies as referred to in the said paragraph 2.	**No equivalent**	**Legal Analysis** The AUC Article 3(1)(e) which includes the creation of and downloading racist and xenophobic material through a computer system rather than merely disseminating or making such material available - but does not include an intent or "*without right*" – the BC language is to be preferred. **Gap Analysis** **Recommendation:** Use the BC language in Article 3 Additional Protocol as a guide for national legislation

[313] Article 29(3)(e) AUC no equivalent in CITO

Offences		
International Best Practice	**National Legislation**	**Comments**
Additional Protocol **Article 4[314] – Racist and xenophobic motivated threat** Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: threatening, through a computer system, with the commission of a serious criminal offence as defined under its domestic law, (i) persons for the reason that they belong to a group, distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors, or (ii) a group of persons which is distinguished by any of these characteristics.	**No equivalent**	**Gap Analysis** **Recommendation:** Use the BC language in Article 4 Additional Protocol as a guide for national legislation
Additional Protocol **Article 5[315] - Racist and xenophobic motivated insult** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: insulting publicly, through a computer system, (i) persons for the reason that they belong to a group distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors; or (ii) a group of persons which is distinguished by any of these characteristics.	**No equivalent**	**Gap Analysis** **Recommendation:** Use the BC language in Article 5 Additional Protocol as a guide for national legislation

[314] Article 29(3)(f) AUC no equivalent in CITO

[315] Article 29(3)(g) AUC no equivalent in CITO

Offences		
International Best Practice	**National Legislation**	**Comments**
2. A Party may either: arequire that the offence referred to in paragraph 1 of this article has the effect that the person or group of persons referred to in paragraph 1 is exposed to hatred, contempt or ridicule; or breserve the right not to apply, in whole or in part, paragraph 1 of this article.		
Additional Protocol **Article 6[316] - Denial, gross minimisation, approval or justification of genocide or crimes against humanity** 1. Each Party shall adopt such legislative measures as may be necessary to establish the following conduct as criminal offences under its domestic law, when committed intentionally and without right: distributing or otherwise making available, through a computer system to the public, material which denies, grossly minimises, approves or justifies acts constituting genocide or crimes against humanity, as defined by international law and recognised as such by final and binding decisions of the International Military Tribunal, established by the London Agreement of 8 August 1945, or of any other international court established by relevant international instruments and whose jurisdiction is recognised by that Party.	**No equivalent**	**Gap Analysis** **Recommendation:** Use the BC language in Article 6 Additional Protocol as a guide for national legislation

[316] Article 29(3)(h) AUC no equivalent in CITO

<table>
<tr><th colspan="3">Offences</th></tr>
<tr><th>International Best Practice</th><th>National Legislation</th><th>Comments</th></tr>
<tr><td>2. A Party may either
a. require that the denial or the gross minimisation referred to in paragraph 1 of this article is committed with the intent to incite hatred, discrimination or violence against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors, or otherwise
b. reserve the right not to apply, in whole or in part, paragraph 1 of this article.</td><td></td><td></td></tr>
<tr><th colspan="3">Additional Offences to Review</th></tr>
<tr><td><b>Identity-related Crimes</b>
<b>Section 14 HIPCAR</b>
A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification by using a computer system in any stage of the offence, intentionally transfers, possesses, or uses, without lawful excuse or justification, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a crime, commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.</td><td></td><td><b>Legal Analysis</b>
This offence covers the preparation phase of an identity –related crime of dishonesty
<b>Gap Analysis</b>
<b>Recommendation:</b> Inclusion in domestic legislation is advisable.</td></tr>
</table>

Offences		
International Best Practice	**National Legislation**	**Comments**
Disclosure of Details of an Investigation **Section 16 HIPCAR** An Internet service provider who receives an order related to a criminal investigation that explicitly stipulates that confidentiality is to be maintained or such obligation is stated by law and intentionally without lawful excuse or justification or in excess of a lawful excuse or justification discloses: • the fact that an order has been made; or • anything done under the order; or • any data collected or recorded under the order; commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.		**Legal Analysis** This offence sanctions data breaches and disclosure of sensitive information that could impact criminal investigations **Gap Analysis** **Recommendation:** Inclusion in domestic legislation is advisable.
Failing to Permit Assistance **Section 17 HIPCAR** 1. A person other than the suspect who intentionally fails without lawful excuse or justification or in excess of a lawful excuse or justification to permit or assist a person based on an order as specified by sections 20 to 22[317] commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. 2. A country may decide not to criminalize the failure to permit assistance provided that other effective remedies are available.		**Legal Analysis** This offence relates to persons, with specific knowledge of relevant evidence, who refuse to assist. Often law enforcement will be reliant upon such persons to secure evidence in cyber investigations. A separate offence is the failure to provide passwords or access to codes to encrypted devices or data (i.e. *"key to protected information"*) – section 53 of the UK Regulation of Investigatory Powers Act 2000 (RIPA) [318] provides for a criminal offence for persons who fail to comply with a section 49 RIPA Notice to disclose the *"key"* **Gap Analysis** **Recommendation:** Inclusion in domestic legislation is advisable.

[317] Search and seizure, assistance and production orders

[318] http://www.legislation.gov.uk/ukpga/2000/23/section/53

Offences		
International Best Practice	**National Legislation**	**Comments**
Cyber Stalking **Section 18 HIPCAR** A person, who without lawful excuse or justification or in excess of a lawful excuse or justification initiates any electronic communication, with the intent to coerce, intimidate, harass, or cause substantial emotional distress to a person, using a computer system to support severe, repeated, and hostile behavior, commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.		**Legal Analysis** This offence criminalizes those who harass persons online– some jurisdictions may have non-computer related harassment offences – but this offence is recommended for those crimes committed online. **Gap Analysis** **Recommendation:** Inclusion in domestic legislation is advisable.
Grooming Children Online **Dutch Criminal Code 248e** The person who proposes to arrange a meeting, by means of an automated work or by making use of a communication service, to a person of whom he knows, or should reasonably assume, that such person has not yet reached the age of sixteen, with the intention of committing indecent acts with this person or of creating an image of a sexual act in which this person is involved, will be punished with a term of imprisonment of at most two years or a fine of the fourth category, if he undertakes any action intended to realise that meeting. **Canadian Criminal Code** **Section 172.1** 1. Every person commits an offence who, by a means of telecommunication, communicates with		**Legal Analysis** To prove the Dutch offence a meeting for sexual purposes is required with supporting evidence of online chat history with sexual intent; request for a meeting with evidence this was planned (i.e. date and place). The purpose of the Canadian law is to prevent grooming by predatory adults of children online. This offence does not require the sexual offence to have occurred. This means the accused does not need to have actually gone to meet the victim in person. The offence is committed before any actions are taken to commit the substantive offence. Article 503-2 of the Criminal Code criminalises any person who *"provokes, incites or facilitates the exploitation of children under 18 in* ***pornography****"* The Dutch and Canadian offences relate to the grooming of children online with a view to committing a sexual act. This is different to the Article 503-2 Criminal Code offence which relates exclusively to pornography. **Gap Analysis** **Recommendation:** Inclusion in domestic legislation is advisable to criminalise this preparatory behaviour before a sexual offence is committed

Offences		
International Best Practice	National Legislation	Comments
a. a person who is, or who the accused believes is, under the age of 18 years, for the purpose of facilitating the commission of an offence under subsection 153(1), section 155, 163.1, 170 or 171 or subsection 212(1), (2), (2.1) or (4) with respect to that person; b. a person who is, or who the accused believes is, under the age of 16 years, for the purpose of facilitating the commission of an offence under section 151 or 152, subsection 160(3) or 173(2) or section 271, 272, 273 or 280 with respect to that person; or c. a person who is, or who the accused believes is, under the age of 14 years, for the purpose of facilitating the commission of an offence under section 281 with respect to that person. Punishment 2. Every person who commits an offence under subsection (1) is guilty of a. is guilty of an indictable offence and is liable to imprisonment for a term of not more than 10 years and to a minimum punishment of imprisonment for a term of one year; or b. is guilty of an offence punishable on summary conviction and is liable to imprisonment for a term of not more than 18 months and to a minimum punishment of imprisonment for a term of 90 days.		

Offences		
International Best Practice	**National Legislation**	**Comments**
Presumption re age 3. Evidence that the person referred to in paragraph (1)(a), (b) or (c) was represented to the accused as being under the age of eighteen years, sixteen years or fourteen years, as the case may be, is, in the absence of evidence to the contrary, proof that the accused believed that the person was under that age. No defence 4. It is not a defence to a charge under paragraph (1)(a), (b) or (c) that the accused believed that the person referred to in that paragraph was at least eighteen years of age, sixteen years or fourteen years of age, as the case may be, unless the accused took reasonable steps to ascertain the age of the person.		

Procedure		
International Best Practice	**National Legislation**	**Comments**
Article 19 BC[319] **Search and seizure of** **stored computer data** 1. 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a. a computer system or part of it and computer data stored therein; and b. a computer-data storage medium in which computer data may be stored in its territory.	**Code of Criminal Procedure** **Articles 57, 59, 60, 62 and 99**	**Legal Analysis** Articles 57 and 59 of the Code of Criminal Procedure allow judicial police officers aware of a felony or flagrante delicto to immediately inform the public prosecutor's office, go to the place where it was committed, and note all the relevant facts. The public prosecutor ensures that the evidence at risk of disappearing and any other element useful in ascertaining the truth are preserved. This includes seizing the instruments used or intended to be used to commit the offence i.e. a computer.

[319] Article 3 AUC

Procedure		
International Best Practice	**National Legislation**	**Comments**
2. Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a. seize or similarly secure a computer system or part of it or a computer-data storage medium; b. make and retain a copy of those computer data; c. maintain the integrity of the relevant stored computer data; d. render inaccessible or remove those computer data in the accessed computer system.		If the nature of the felony or misdemeanor is such that the evidence may be acquired through the seizing of papers, documents, other objects in the possession of the persons who may have been involved in the offence, or other evidence or objects related to the offence, judicial police officers may go immediately to their place of residence to conduct a search, which is transcribed in a report, in accordance with Articles 60 and 62. Except in matters of harm to State security or terrorist offences, the judicial police officer only, with the persons designated in Article 60, is authorized to take note of the papers or documents prior to their seizure. In case of search at the premises of a person subjected to professional secrecy by law, the judicial police officer has the obligation to notify the competent public prosecutor and to adopt all the measures to ensure that the respect for professional secrecy is guaranteed beforehand. Where appropriate, the judicial police officer can take fingerprints at the place of the offence and may request expert assessments on the instruments used to commit the offence and on the objects discovered and seized at the place of the offence or with the suspects. Pursuant to Article 99 of the Code of Criminal Procedure, the investigating judge may enter the place in order to note all the relevant facts or conduct a search. They shall notify the public prosecutor's office and the latter's representative may accompany them.

Procedure		
International Best Practice	National Legislation	Comments
4. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2. 5. The powers and procedures referred to in this article shall be subject to Articles 14 and 15. **Section 20 HIPCAR – Search and Seizure** 1. If a [judge] [magistrate] is satisfied on the basis of [information on oath] [affidavit] that there are reasonable grounds [to suspect] [to believe] that there may be in a place a thing or computer data: a. that may be material as evidence in proving an offence; or b. that has been acquired by a person as a result of an offence; the [judge] [magistrate] [may] [shall] issue a warrant authorizing a [law enforcement] [police] officer, with such assistance as may be necessary, to enter the place to search and seize the thing or computer data including search or similarly access: i. a computer system or part of it and computer data stored therein; and		**Gap Analysis** **Recommendation:** This is the most essential investigatory power and should refer to gaining access than search. In the BC Explanatory Report, *"Search"* means to seek, read, inspect or review data. Articles 60 and 62 do not refer to "data" and is not computer specific. It can be essential in cybercrime investigations to access the computer and the data contained therein. The Code of Criminal Procedure does not make it clear if stored computer data per se will be considered as a tangible object and therefore seized in a parallel manner as tangible objects such as computers, other than by securing the computer or data medium upon which it is stored. The Code of Criminal Procedure relates to the seizure of documents or records and a search gathering evidence that has been recorded or registered in the past in tangible form, such as ink on paper. Cyber investigators need to search, inspect or access data, and seize or physically take it away. necessary in order to ensure that computer data can be obtained in a manner that is equally effective as a search and seizure of a tangible object containing the data, such as a computer. This is important to ensure the integrity and provenance of the data. There are several factors to consider in any legislation: first, the data is in intangible form, such as in an electromagnetic form. Second, while the data may be read with the use of computer equipment, it cannot be seized and taken away in the same sense as can a paper record. The physical medium on which the intangible data is stored (e.g., the computer hard-drive or a diskette) must be seized and taken away, or a copy of the data must be made in either tangible form (e.g., computer print-out) or intangible form, on a physical medium (e.g., diskette), before the tangible medium containing the copy can be seized and taken away. In the latter two situations, where such copies of the data are made, a copy of the data remains in the computer system or storage device.

Procedure		
International Best Practice	**National Legislation**	**Comments**
ii. a computer-data storage medium in which computer data may be stored in the territory of the country. 2. If [law enforcement] [police] officer that is undertaking a search based on Sec. 20 (1) has grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, he shall be able to expeditiously extend the search or similar accessing to the other system. 3. A [law enforcement] [police] officer that is undertaking a search are empowered to seize or similarly secure computer data accessed according to paragraphs 1 or 2. **Section 21 HIPCAR – Assistance** Any person who is not a suspect of a crime but who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein that is the subject of a search under section 20 must permit, and assist if reasonably required and requested by the person authorized to make the search by: • providing information that enables the undertaking of measures referred to in section 20;		Further, additional procedural provisions are Domestic law should provide for a power to make such copies. Third, due to the connectivity of computer systems, data may not be stored in the particular computer that is searched, but such data may be readily accessible to that system. It could be stored in an associated data storage device that is connected directly to the computer, or connected to the computer indirectly through communication systems, such as the Internet. This may or may not require new laws to permit an extension of the search to where the data is actually stored (or the retrieval of the data from that site to the computer being searched), or the use of traditional search powers in a more co-ordinated and expeditious manner at both locations. The word *"access"* is important as this has a neutral meaning and reflects more accurately computer terminology – this is also used in Articles 26-27 of CITO.[320] The national legislation could incorporate relevant language from BC and HIPCAR to include definitions of a computer system[321] and computer data[322] and refer consistently to *access* There should be a definition of "*seize*" to insure integrity and to specific procedures - section 3(16) HIPCAR "*Seize includes:* • *activating any onsite computer system and computer data storage media;* • *making and retaining a copy of computer data, including by using onsite equipment;* • *maintaining the integrity of the relevant stored computer data;* • *rendering inaccessible, or removing, computer data in the accessed computer system;* • *taking a printout of output of computer data; or* • *seize or similarly secure a computer system or part of it or a computer- data storage medium."*

[320] Paragraphs 184-191 pages 31- 33 Explanatory Report BC

[321] See Article 1.a. BC: "*any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data*" **or** section 3(5) HIPCAR: "*a device or a group of inter-connected or related devices, including the Internet, one or more of which, pursuant to a program, performs automatic processing of data or any other function.*"

[322] See Article 1.b. BC: "*any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function*" **or** section 3(6) HIPCAR: "*Computer data means any representation of facts, concepts, information (being either texts, sounds or images) machine-readable code or instructions, in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.*"

Procedure		
International Best Practice	**National Legislation**	**Comments**
• accessing and using a computer system or computer data storage medium to search any computer data available to or in the system; • obtaining and copying such computer data; • using equipment to make copies; and • obtaining an intelligible output from a computer system in such a format that is admissible for the purpose of legal proceedings. **Article 26 CITO - Inspecting Stored Information** 1. Every State Party shall commit itself to adopting the procedures necessary to enable its competent authorities to inspect or access: a. an information technology or part thereof and the information stored therein or thereon. b. the storage environment or medium in or on which the information may be stored. 2. Every State Party shall commit itself to adopting the procedures necessary to enable the competent authorities to inspect or access a specific information technology or part thereof in conformity with paragraph 1(a) if it is believed that the required information is stored in another information technology or in part thereof in its territory and such information is legally accessible or available in the first technology, the scope of inspection may be extended and the other technology accessed.		Section 21 HIPCAR provides for legislation to ensure assistance is provided by those who have specialist knowledge of the location of relevant evidence – this could be used as a guide – also see section 17 HIPCAR for an offence if assistance is refused without lawful excuse

Procedure		
International Best Practice	National Legislation	Comments
Article 27 CITO - Seizure of Stored Information 1. Every State Party shall commit itself to adopting the procedures necessary to enable the competent authorities to seize and safeguard information technology information accessed according to Article 26, paragraph 1, of this Convention. These procedures include the authority to: a. seize and safeguard the information technology or part thereof or the storage medium for the information technology information. b. make a copy the information technology information and keep it. c. maintain the integrity of the stored information technology information. d. remove such accessed information from the information technology or prevent its access. 2. Every State Party shall commit itself to adopting the procedures necessary to enable the competent authorities to order any person who is acquainted with the functioning of the information technology or the procedures applied to protect the information technology to give the information necessary to complete the procedures mentioned in paragraphs 2 and 3 of Article 26 of this Convention.		

Procedure		
International Best Practice	**National Legislation**	**Comments**
Article 16 BC[323] **Expedited preservation of stored computer data** 1. Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2. Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.	**No equivalent**	**Legal Analysis** This procedural power is important to ensure that data which is vulnerable to deletion or loss is preserved **Gap Analysis** **Recommendation:** This expedited power to retain BSI, metadata, transactional and stored content is essential as part of cybercrime investigations to ensure the evidence is available for search, access, seizure and review. The language of Article 16 of the BC, section 23 HIPCAR or Article 23 CITO could be used. This will also require definitions of *"computer data"*,[324] *"subscriber information or BSI"*, *"traffic data"*[325] and *"Communication Service Provider"*[326] To note BC and HIPCAR do not provide a definition of BSI – but CITO does for subscriber information:[327] *"Any information that the service provider has concerning the subscribers to the service, except for information through which the following can be known:* a. *The type of communication service used, the technical requirements and the period of service.* b. *The identity of the subscriber, his postal or geographic address or phone number and the payment information available by virtue of the service agreement or arrangement* c. *Any other information on the installation site of the communication equipment by virtue of the service agreement."* Consideration should be given the length of preservation that is reasonable in the circumstances and allowing for an application to extend in exigent circumstances – BC and CITO have 90 days and HIPCAR 7 days. From experience 90 days is too few in a cyber investigation and the figure should be nearer 180 days and then subject to extension.

[323] no equivalent in AUC

[324] See Article 1.b. BC **or** section 3(6) HIPCAR

[325] See Article 1.d BC: "*any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service*" **or** section 3(18) HIPCAR: "*Traffic data means computer data that: a. relates to a communication by means of a computer system; and b. is generated by a computer system that is part of the chain of communication ; and c. shows the communication's origin, destination, route, time date, size, duration or the type of underlying services.*"

[326] See Article 1.c. BC: "*i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii any other entity that processes or stores computer data on behalf of such communication service or users of such service.*"

[327] See Article 2(9) CITO

Procedure		
International Best Practice	**National Legislation**	**Comments**
3. Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. 4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15. **Section 23 HIPCAR – Expedited Preservation** If a [law enforcement] [police] officer is satisfied that there are grounds to believe that computer data that is reasonably required for the purposes of a criminal investigation is particularly vulnerable to loss or modification, the [law enforcement] [police] officer may, by written notice given to a person in control of the computer data, require the person to ensure that the data specified in the notice be preserved for a period of up to seven (7) days as specified in the notice. The period may be extended beyond seven (7) days if, on an ex parte application, a [judge] [magistrate] authorizes an extension for a further specified period of time. **Article 23 CITO - Expeditious Custody of Data Stored in Information Technology** 1. Every State Party shall adopt the procedures necessary to enable the competent authorities to issue orders or obtain the expeditious custody of information, including information for tracking users, that was stored on an information technology, especially if it is believed that such information could be lost or amended.		

Procedure		
International Best Practice	**National Legislation**	**Comments**
2. Every State Party shall commit itself to adopting the procedures necessary as regards paragraph 1, by means of issuing an order to a person to preserve the information technology information in his possession or under his control, in order to require him to preserve and maintain the integrity of such information for a maximum period of 90 days that may be renewed, in order to allow the competent authorities to search and investigate 3. Every State Party shall commit itself to adopting the procedures necessary to require the person responsible for safeguarding the information technology to maintain the procedures secrecy throughout the legal period stated in the domestic law.		
Article 17 BC[328] **Expedited preservation and partial disclosure of traffic data** 1. Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to: a. ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and	**No equivalent**	**Legal Analysis** This procedural power is especially important to ensure that CSPs provide IP addresses that could locate the perpetrator of a cybercrime. **Gap Analysis** **Recommendation:** This expedited power alongside disclosure of traffic data should be included in legislation to enable effective investigations of cybercrime. The language of Article 17 of the BC, sections 23 and 24 HIPCAR or Article 24 CITO could be used. This will also require definitions of *"traffic data"* and *"Communication Service Provider"*[329]

[328] no equivalent in AUC
[329] See definitions above

Procedure		
International Best Practice	National Legislation	Comments
b. ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted. 2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15. **Section 23 HIPCAR – Expedited Preservation** If a [law enforcement] [police] officer is satisfied that there are grounds to believe that computer data that is reasonably required for the purposes of a criminal investigation is particularly vulnerable to loss or modification, the [law enforcement] [police] officer may, by written notice given to a person in control of the computer data, require the person to ensure that the data specified in the notice be preserved for a period of up to seven (7) days as specified in the notice. The period may be extended beyond seven (7) days if, on an ex parte application, a [judge] [magistrate] authorizes an extension for a further specified period of time.		

Procedure		
International Best Practice	National Legislation	Comments
Section 24 HIPCAR – Partial Disclosure of Traffic Data If a [law enforcement] [police] officer is satisfied that data stored in a computer system is reasonably required for the purposes of a criminal investigation, the [law enforcement] [police] officer may, by written notice given to a person in control of the computer system, require the person to disclose sufficient traffic data about a specified communication to identify: a. the Internet service providers; and/or b. the path through which the communication was transmitted. **Article 24 CITO - Expeditious Custody and Partial Disclosure of Users Tracking Information** Every State Party shall commit itself to adopting the procedures necessary as regards users tracking information in order to: 1. ensure expeditious custody of users tracking information, regardless of whether such communication is transmitted by one or more service providers. 2. ensure that a sufficient amount of users tracking information is disclosed to the competent authorities of the State Party or to a person appointed by these authorities to allow the State Party to determine the service providers and the transmission path of the communications.		

Procedure		
International Best Practice	**National Legislation**	**Comments**
Article 18 BC[330] **Production Order** 1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a. a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and b. a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. 2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 3. For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a. the type of communication service used, the technical provisions taken thereto and the period of service;	**No equivalent**	**Legal Analysis** This is an essential provision for an effective cybercrime investigation and its absence will impact upon prosecutions and international cooperation. **Gap Analysis** **Recommendation:** This essential power is necessary to ensure CSPs in Morocco provide BSI, traffic data and stored content data. This will also require definitions of *"computer data", "subscriber information or BSI", "traffic data"* and *"Communication Service Provider"*.[331] Article 25 CITO is a model that could be used and uses different definitions including *"information technology",*[332] *"service provider"*[333] and *"data"*[334] – it is still advisable to have definitions for *"subscriber information or BSI", "traffic data"* as they will be different types of evidence that can be produced from CSPs. Further, this power will require individuals and others (such as corporate entities, financial institutions and other organisations) who hold data to produce it to law enforcement authorities. Article 18 BC and section 22 HIPCAR could be a guide with consistent application of definitions

[330] no equivalent in AUC

[331] See definitions above

[332] Article 2(1) CITO: "*any material or virtual means or group of interconnected means used to store, sort, arrange, retrieve, process, develop and exchange information according to commands and instructions stored therein. This includes all associated inputs and outputs, by means of wires or wirelessly, in a system or network.*"

[333] Article 2(2) CITO: "*any natural or juridical person, common or private, who provides subscribers with the services needed to communicate through information technology, or who processes or stores information on behalf of the communication service or its users.*"

[334] Article 2(3) CITO: "*all that may be stored, processed, generated and transferred by means of information technology, such as numbers, letters, symbols, etc…*"

Procedure		
International Best Practice	National Legislation	Comments
b. the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c. c.any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement. **Section 22 HIPCAR – Production Order** If a [judge] [magistrate] is satisfied on the basis of an application by a [law enforcement] [police] officer that specified computer data, or a printout or other information, is reasonably required for the purpose of a criminal investigation or criminal proceedings, the [judge] [magistrate] may order that: • a person in the territory of [enacting country] in control of a computer system produce from the system specified computer data or a printout or other intelligible output of that data; or • an Internet service provider in [enacting country] to produce information about persons who subscribe to or otherwise use the service. **Article 25 CITO - Order to Submit Information** Every State Party shall commit itself to adopting the procedures necessary to enable the competent authorities to issue orders to:		

Procedure		
International Best Practice	**National Legislation**	**Comments**
1. Any person in its territory to submit certain information in his possession which is stored on information technology or a medium for storing information. 2. Any service provider offering his services in the territory of the State Party to submit user's information related to that service which is in the possession of the service provider or under his control.		
Article 21 BC[335] **Interception of content data** 1. Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: a. collect or record through the application of technical means on the territory of that Party, and b. compel a service provider, within its existing technical capability: i. to collect or record through the application of technical means on the territory of that Party, or ii. to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system.	**No equivalent**	**Legal Analysis** This power is essential for national legislation – and there must be safeguards and requirement/procedure to compel CSPs cooperation to collect or record content data in real-time of specific communications in Morocco. **Gap Analysis** **Recommendations:** Provision should be made to compel CSPs in Morocco to cooperate with real-time collection of content; and safeguards should be incorporated to ensure the collection is legal, necessary, reasonable and proportionate in the circumstances. Consideration should be given to reviewing Article 29 of CITO, Article 21 BC and section 26 HIPCAR and incorporating language in national legislation

[335] no equivalent in AUC

Procedure		
International Best Practice	National Legislation	Comments
2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory. 3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15. **Section 26 HIPCAR – Interception of Content Data** 1. If a [judge] [magistrate] is satisfied on the basis of [information on oath] [affidavit] that there are reasonable grounds to [suspect] [believe] that the content of electronic communications is reasonably required for the purposes of a criminal investigation, the magistrate [may] [shall]: • order an Internet service provider whose service is available in [enacting country] through application of technical means to collect or record or to permit or assist competent authorities with the collection or recording of content data associated with specified communications transmitted by means of a computer system; o		

Procedure		
International Best Practice	National Legislation	Comments
- authorize a [law enforcement] [police] officer to collect or record that data through application of technical means. 2. A country may decide not to implement section 26. **Article 29 CITO - Interception of Content Information** 1. Every State Party shall commit itself to adopting the legislative procedures necessary as regards a series of offences set forth in the domestic law, in order to enable the competent authorities to: a. gather or register through technical means in the territory of this State Party, or b. cooperate with and help the competent authorities to expeditiously gather and register content information of the relevant communications in its territory and which are transmitted by means of the information technology. 2. If, because of the domestic legal system, the State Party is unable to adopt the procedures set forth in paragraph 1(a), it may adopt other procedures in the form necessary to ensure the expeditious gathering and registration of content information corresponding to the relevant communications in its territory using the technical means in that territory. 3. Every State Party shall commit itself to adopting the procedures necessary to require the service provider to maintain the secrecy of any information when exercising the authority set forth in this Article.		

Procedure		
International Best Practice	**National Legislation**	**Comments**
Article 20 BC[336] **Real-time collection of traffic data** 1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a. collect or record through the application of technical means on the territory of that Party, and b. compel a service provider, within its existing technical capability: i. to collect or record through the application of technical means on the territory of that Party; or ii. to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.	**No equivalent**	**Legal Analysis** There is no procedural power just to collect traffic data real-time. There could be a lower threshold to collect real-time traffic data which is an essential investigative tool. There may be situations where a higher legal threshold to secure content is not made out by an applicant – but a lower threshold to secure traffic could be. For this reason, there should be a distinction between real-time collection of stored content and traffic data. There must be safeguards and requirements/procedure to compel CSPs cooperation to collect or record content data in real-time of specific communications in Morocco **Gap Analysis** **Recommendations:** There should be a specific power to collect traffic data real-time and provision should be made to compel CSPs in Morocco to cooperate with real-time collection of traffic data; and safeguards should be incorporated to ensure the collection is legal, necessary, reasonable and proportionate in the circumstances. The language from Article 28 CITO could be considered but this does not refer to real-time only expeditious collection. Article 20 BC and section 25 HIPCAR should be used as a guide for national legislation

[336] Article 31(3)(e) AUC - Article 28 CITO refers to expeditious collection rather than real-time collection

Procedure		
International Best Practice	National Legislation	Comments
3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15. **Section 25 HIPCAR - Collection of Traffic Data** 1. If a [judge] [magistrate] is satisfied on the basis of [information on oath][affidavit] that there are reasonable grounds to [suspect] [believe] that traffic data associated with a specified communication is reasonably required for the purposes of a criminal investigation, the [judge] [magistrate] [may] [shall] order a person in control of such data to: a. collect or record traffic data associated with a specified communication during a specified period; or b. permit and assist a specified [law enforcement] [police] officer to collect or record that data. 2. If a [judge] [magistrate] is satisfied on the basis of [information on oath] [affidavit] that there are reasonable grounds to [suspect] [believe] that traffic data is reasonably required for the purposes of a criminal investigation, the [judge] [magistrate] [may] [shall] authorize a [law enforcement] [police] officer to collect or record traffic data associated with a specified communication during a specified period through application of technical means.		

Procedure		
International Best Practice	**National Legislation**	**Comments**
3. A country may decide not to implement section 25.		
		Disclosure obligation of encryption keys With terrorists and organized criminals routinely using encrypted messaging applications[337] this may be considered a viable power to release the keys to passwords to unlock devices[338] **Gap Analysis** **Recommendation:** Unable to clarify if there were any such powers in Morocco – but such a power will allow law enforcement to compel owners to unlock devices
		Data retention obligations[339] Such a power can allow law enforcement to 1. Trace and identify the source of a communication 2. Identify the destination of a communication; 3. Identify the date, time and duration of a communication; and 4. Identify the type of communication Morocco does not have such an obligation[340]

[337] Eleanor Saitta. "Can Encryption Save Us?" Nation 300, no. 24 (June 15, 2015): 16-18. Academic Search Premier, EBSCOhost (accessed February 29, 2016).

[338] For an example see section 49 Regulation of Investigatory Powers Act 2000 (UK) - http://www.legislation.gov.uk/ukpga/2000/23/section/49

[339] In 2006 the EU issued its Data Retention Directive - EU Member States had to store electronic telecommunications data for at least six months and at most 24 months for investigating, detecting and prosecuting serious crime. In 2014, the Court of Justice of the EU invalidated the Data Retention Directive, holding that it provided insufficient safeguards against interferences with the rights to privacy and data protection. In the absence of a valid EU Data Retention Directive, Member States may still provide for a data retention scheme – for national schemes see: http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention

[340] ICMEC Global Review page 33

International Cooperation

International Best Practice	National Legislation	Comments
Article 22 BC **Jurisdiction** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: a. in its territory; or b. on board a ship flying the flag of that Party; or c. on board an aircraft registered under the laws of that Party; or d. by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. 2. Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 3. Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition. 4. This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.	**Code of Criminal Procedure** **Articles 704, 705, 706, 707, 708, 709, 710, 711, 712 and 749**	**Legal Analysis** The Code of Criminal Procedure clearly defines jurisdiction - that will equally apply to cybercrime offences. **Gap Analysis** **Recommendation:** In the case of crimes committed by use of computer systems, there will be occasions in which more than one Party has jurisdiction over some or all of the participants in the crime. For example, many virus attacks, frauds and copyright violations committed through use of the Internet target victims located in more than one State. If there is a conflict between jurisdictions consideration should be given to guidelines on determining the appropriate jurisdiction to try an offence – see the Eurojust Guidelines for Deciding which Jurisdiction should Prosecute (revised 2016)[341]

[341] http://www.eurojust.europa.eu/Practitioners/operational/Documents/Operational-Guidelines-for-Deciding.pdf

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
5. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution. **Section 19 HIPCAR – Jurisdiction** This Act applies to an act done or an omission made: • in the territory of [enacting country]; or • on a ship or aircraft registered in [enacting country]; or • by a national of [enacting country] outside the jurisdiction of any country; or by a national of [enacting country] outside the territory of [enacting country], if the person's conduct would also constitute an offence under a law of the country where the offence was committed. **Article 30 CITO - Competence** 1. Every State Party shall commit itself to adopting the procedures necessary to extend its competence to any of the offences set forth in Chapter II of this Convention, if the offence is committed, partly or totally, or was realized: a. in the territory of the State Party b. on board a ship raising the flag of the State Party. c. on board a plane registered under the law of the State Party. d. by a national of the State Party if the offence is punishable according to the domestic law in the location where it was committed, or if it was committed outside the jurisdiction of any State.		

International Cooperation		
International Best Practice	National Legislation	Comments
e. if the offence affects an overriding interest of the State. 2. Every State Party shall commit itself to adopting the procedures necessary to extend the competence covering the offences set forth in Article 31, paragraph 1, of this Convention in the cases in which the alleged offender is present in the territory of that State Party and shall not extradite him to another Party according to his nationality following the extradition request. 3. If more than one State Party claim to have jurisdiction over an offence set forth in this Convention, priority shall be accorded to the request of the State whose security or interests were disrupted by the offence, followed by the State in whose territory the offence was committed, and then by the State of which the wanted person is a national. In case of similar circumstances, priority shall be accorded to the first State that requests the extradition.		

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
Article 35 BC[342] **24/7 Network** 1. Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures: a. the provision of technical advice; b. the preservation of data pursuant to Articles 29 and 30; c. the collection of evidence, the provision of legal information, and locating of suspects. 2. a. A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis. b. If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to coordinate with such authority or authorities on an expedited basis. 3. Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.	**No equivalent**	**Legal Analysis** This is an essential mechanism for an effective cybercrime investigative capability and a requirement of the BC. **Gap Analysis** **Recommendation:** This should not require legislation to implement and subject to resources should be established as a priority. Contact details should be shared for the nominated single point of contact (SPOC) nationally, central authorities internationally and INTERPOL. Consideration should also be given to drafting a Memorandum of Understanding with national agencies so that the SPOC has authority to undertake the actions required as part of an international cybercrime investigation applying national laws and treaties. This MOU will include both incoming and outgoing requests and ensure an efficient and effective process.

[342] Article 43 CITO

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
Article 25 BC **General principles relating to mutual assistance** 1. The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. 2. Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35. 3. Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.		**Legal Analysis** Article 25 BC ensures that the BC can be used as an instrument to facilitate MLA. Morocco has ratified the BC and this will be the basis for cooperation with other States that have ratified. Without national legislation requests cannot be made by non-BC States for expedited preservation of stored computer data, expedited preservation and partial disclosure of traffic data and disclosure of stored data and traffic data, meaning a limitation to the international cooperation that Morocco can provide to Requesting States. **Gap Analysis** **Recommendation:** Domestic law is required for expedited preservation of stored computer data, expedited preservation and partial disclosure of traffic data and production orders. The BC can be used as precedents for expedited preservation of stored computer data,[343] expedited preservation and partial disclosure of traffic data[344] and disclosure of stored data345 and traffic data[346] . Consideration should be given to allowing adjudicating authorities to authorise domestic law enforcement to investigate in the State where access to a device is known. Accessibility of information is the essential criterion to initiate an investigation in cases where it is not possible to know where the data is stored (i.e. in the cloud). This could include a *"mutual recognition"* of court orders issued towards communication service providers in a given State, that could be served to branches of that CSPs located in other States, depending on where the data is stored.

[343] Article 29 BC

[344] Article 30 BC

[345] Article 31 BC

[346] Article 33 BC

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
4. Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence. 5. Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.		

International Cooperation		
International Best Practice	National Legislation	Comments
Article 34 CITO - Procedures for Cooperation and Mutual Assistance Requests 1. The provisions of paragraphs 2-9 of this Article shall apply in case no cooperation and mutual assistance treaty or convention exists on the basis of the applicable legislation between the State Parties requesting assistance and those from which assistance is requested. If such a treaty or convention exists, the mentioned paragraphs shall not apply, unless the concerned parties agree to apply them in full or in part. 2. a. Every State Party shall designate a central authority responsible for sending and responding to mutual assistance requests and for their implementation and referral to the relevant authorities for implementation. b. Central authorities shall communicate directly among themselves. c. Every State Party shall, at the time of signature or deposit of the instrument of ratification, acceptance or agreement, contact the General Secretariat of the Council of Arab Interior Ministers and the Technical Secretariat of the Arab Justice Ministers and communicate to them the names and addresses of the authorities specifically designated for the purposes of this paragraph.		

International Cooperation		
International Best Practice	National Legislation	Comments
d. The General Secretariat of the Council of Arab Interior Ministers and the Technical Secretariat of the Arab Justice Ministers shall establish and update a registry of concerned central authorities appointed by the State Parties. Every State Party shall insure that the registry's details are correct at all times 3. Mutual assistance requests in this Article shall be implemented according to procedures specified by the requesting State Party, except in the case of non conformity with the law of the State Party from which assistance is requested. 4. The State Party from which assistance is requested may postpone taking action on the request if such action shall affect criminal investigations conducted by its authorities. 5. Prior to refusing or postponing assistance, the State Party from which assistance is requested shall decide, after consulting with the requesting State Party, whether the request shall be partially fulfilled or be subject to whatever conditions it may deem necessary. 6. The State Party from which assistance is requested shall commit itself to inform the requesting State Party of the result of the implementation of the request. If the request is refused or postponed, the reasons of such refusal or postponement shall be given. The State Party from which assistance is requested shall inform the requesting State Party of the reasons that prevent the complete fulfilment of the request or the reasons for its considerable postponement.		

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
7. The State Party requesting assistance may request the State Party from which assistance is requested to maintain the confidentiality of the nature and content of any request covered by this chapter, except in as far as necessary to implement the request. If the State Party from which assistance is requested cannot abide by this request concerning confidentiality, it shall so inform the requesting State Party which will then decide about the possibility of implementing the request. 8. a. In case of emergency, mutual assistance requests may be sent directly to the judicial authorities in the State Party from which assistance is requested from their counterparts in the requesting State Party. In such case, a copy shall be sent concurrently from the central authority in the requesting State Party to its counterpart in the State Party from which assistance is requested. b. Communications can be made and requests submitted pursuant to this paragraph through INTERPOL. c. Whenever, according to paragraph a, a request is submitted to an authority, but that authority is not competent to deal with that request, it shall refer the request to the competent authority and directly inform the requesting State Party accordingly.		

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
d. Communications and requests carried out according to this paragraph and not concerning compulsory procedures may be transmitted directly by the competent authorities in the requesting State Party to their counterpart in the State Party from which assistance is requested. e. Every State Party may, at the time of signature, ratification, acceptance or adoption, inform the General Secretariat of the Council of Arab Interior Ministers and the Technical Secretariat of the Arab Justice Ministers that requests according to this paragraph must be submitted to the central authority for reasons of efficiency.		
Article 26 BC **Spontaneous Information** 1. A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.		**Legal Analysis** This is an important procedure to enable a state privy to information that will assist another state to prevent a cybercrime or to investigate it. Albeit available between CITO ratified states in CITO Article 33, Morocco has no domestic legal basis to share such information with non-CITO states unless an official request is sent through the usual MLA channels.

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
2. Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them. **Article 33 CITO - Circumstantial Information** 1. A State Party may – within the confines of its domestic law – and without prior request, give another State information it obtained through its investigations if it considers that the disclosure of such information could help the receiving State Party in investigating offences set forth in this convention or could lead to a request for cooperation from that State Party. 2. Before giving such information, the State Party providing it may request that the confidentiality of the information be kept; if the receiving State Party cannot abide by this request, it shall so inform the State Party providing the information which will then decide about the possibility of providing the information. If the receiving State Party accepts the information on condition of confidentiality, the information shall remain between the two sides.	**No equivalent**	Article 18(4)-(5) UNTOC provides for the sharing of intelligence spontaneously for matters fulfilling the definition of a serious crime[347], that is transnational[348] and involves an organized crime group[349]. Without satisfying this definition an official request will need to be sent through the usual MLA channels to non-CITO states. On the basis of the fast-moving nature of cybercriminality spontaneous sharing is an effective way to cooperate with other states and its absence inhibits effective international collaboration with non-CITO states. **Gap Analysis** **Recommendation:** Use UNTOC Article 18(4)-(5) as the basis to spontaneously share information that fulfils the scope of UNTOC (with guarantees provided about use in evidence or disclosure of sensitive information to a third party (including another state).[350] Consider legislation based on Article 33 CITO or Article 26 BC.

[347] Article 2(b) UNTOC ““*Serious crime” shall mean conduct constituting an offence punish- able by a maximum deprivation of liberty of at least four years or a more serious penalty*”

[348] Article 3(1) UNTOC

[349] Article 2(a) UNTOC ““*Organized criminal group” shall mean a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit*”

[350] See Article 33(2) CITO

International Cooperation		
International Best Practice	National Legislation	Comments
Article 32 BC **Trans-border access to stored computer data with consent or where publicly available** A Party may, without the authorisation of another Party: a. access publicly available (open source) stored computer data, regardless of where the data is located geographically; or b. access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system. **Section 27 HIPCAR – Forensic Software** 1. If a [judge] [magistrate] is satisfied on the basis of [information on oath] [affidavit] that in an investigation concerning an offence listed in paragraph 7 herein below there are reasonable grounds to believe that essential evidence cannot be collected by applying other instruments listed in Part IV but is reasonably required for the purposes of a criminal investigation, the [judge] [magistrate] [may] [shall] on application authorize a [law enforcement] [police] officer to utilize a remote forensic software with the specific task required for the investigation and install it on the suspect's computer system in order to collect the relevant evidence. The application needs to contain the following information:		**Legal Analysis** This procedural power enables a state to secure content stored in another state in limited circumstances. Article 32.b. BC and Article 40 CITO is an exception to the principle of territoriality and permits unilateral trans-border access without the need for mutual legal assistance where there is consent or the information is publicly available. Examples of use of this procedural power under BC Article 32.b. include: A person's e-mail may be stored in another country by a service provider, or a person may intentionally store data in another country. These persons may retrieve the data and, provided that they have the lawful authority, they may voluntarily disclose the data to law enforcement officials or permit such officials to access the data[351] A suspected terrorist is lawfully arrested while his/her mailbox – possibly with evidence of a crime – is open on his/her tablet, smartphone or other device. If the suspect voluntarily consents that the police access the account and if the police are sure that the data of the mailbox is located in another state, police may access the data under Article 32.b. **Gap Analysis** **Recommendation:** This restricted power to unilaterally secure evidence is included in legislation with safeguards to ensure the consent is lawfully obtained from the user.[352] Language can be used from Article 32 BC and Article 40 CITO. Article 32.b. has been heavily criticized and it may be considered that the consent of the state where the stored computer data is stored is obtained in addition to the user. Section 27 HIPCAR provides for forensic software and this may allow access to a computer in another state. There are a number of restrictions that requires the evidence cannot be obtained by other means, a judicial order is required, can only apply to certain offences and is for a restricted period (3 months). Consideration should also be given to consent of the other state where the forensic software may intrude.

[351] Paragraph 294, page 53 BC Explanatory Report

[352] Consideration should be given to situations such as the non-availability of a user (e.g. death) and if consent can be obtained in another state

International Cooperation		
International Best Practice	National Legislation	Comments
• suspect of the offence, if possible with name and address; and • description of the targeted computer system; and • description of the intended measure, extent and duration of the utilization; and • reasons for the necessity of the utilization. 2. Within such investigation it is necessary to ensure that modifications to the computer system of the suspect are limited to those essential for the investigation and that any changes if possible can be undone after the end of the investigation. During the investigation, it is necessary to log • the technical mean used and time and date of the application; and • the identification of the computer system and details of the modifications undertaken within the investigation; any information obtained. Information obtained by the use of such software needs to be protected against any modification, unauthorized deletion and unauthorized access. 3. The duration of authorization in section 27 (1) is limited to [3 months]. If the conditions of the authorization is no longer met, the action taken are to stop immediately. 4. The authorization to install the software includes remotely accessing the suspects computer system. 5. If the installation process requires physical access to a place the requirements of section 20 need to be fulfilled.		

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
6. If necessary a [law enforcement] [police] officer may pursuant to the order of court granted in (1) above request that the court order an internet service provider to support the installation process. 7. [List of offences]. 8. A country may decide not to implement section 27. **Article 40 CITO - Access to Information Technology Information Across Borders** A State Party may, without obtaining an authorization from another State Party: 1. Access information technology information available to the public (open source), regardless of the geographical location of the information. 2. Access or receive – through information technology in its territory – information technology information found in the other State Party, provided it has obtained the voluntary and legal agreement of the person having the legal authority to disclose information to that State Party by means of the said information technology.	**No equivalent**	

Palestine

The Palestinian Authority (PA) has ratified CITO and on July 9 2017, Law No. 16 of 2017 on Electronic Crimes was issued.[353]

Offences		
International Best Practice	**National Legislation**	**Comments**
Article 2 BC – Illegal access Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system. **Article 6 CITO – Illicit Access** 1. Illicit access to, presence in or contact with part or all of the information technology, or the perpetuation thereof. 2. The punishment shall be increased if this access, presence, contact or perpetuation leads to: a. the obliteration, modification, distortion, duplication, removal or destruction of saved data, electronic instruments and systems and communication networks, and damages to the users and beneficiaries. b. the acquirement of secret government information.	**Law No.16 of 2017 on Electronic Crimes** **Article 4(1)**	**Legal Analysis** Article 4(1) is consistent with Article 6 CITO which refers to *"illicit access to, presence in or contact with"* without defining what these acts mean. BC refers to *"without right"* in Article 2 on the basis the access is unauthorized. The BC Explanatory Report confirmed the derivation of *"without right"* as, *"conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law."* Article 4(1) of the national law also includes an offence of illegal remaining. The national legislation does not include programs within the definition of *"data"* **Gap Analysis** **Recommendation:** The national legislation could incorporate the inclusion of programs within the definition of data as some data includes programs and other data does not. Further, the national legislation could a provide a definition of *"illicit access"* to ensure it is only an offence without justification or reasonable excuse. This is the reason for the BC including *"without right"* and ensures, for example, that law enforcement officials can access a computer system where justified for an investigation.

[353] The text is only available in Arabic

Offences		
International Best Practice	**National Legislation**	**Comments**
Article 3 BC **Illegal Interception** Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system. **Article 7 CITO** **Illicit Interception** The deliberate unlawful interception of the movement of data by any technical means, and the disruption of transmission or reception of information technology data.	**Law No.16 of 2017 on Electronic Crimes** **Article 7**	**Legal Analysis** This offence is essential to prosecute transmissions of computer data to, from, or within a computer system that may be illegally intercepted to obtain information (e.g. wikileaks or Panama Papers). **Gap Analysis** **Recommendation:** *I*t is understood that language from Article 7 CITO has been used – CITO does not contain a definition of *"information technology data"* and this needs to be incorporated as deemed to be distinct to data. The national legislation could have a definition of data or computer data only - Article 3 BC refers to interception of *"computer data"* which is defined in Article 1.b BC as "any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service."
Article 4 BC **Data Interference** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.		**Legal Analysis** If the same language is used for the national legislation, as referred to in CITO, no reference is made to *"without right."* Further, CITO does not include suppression of computer data, which is an element of phishing to obtain illegal access by installing a keylogger to obtain sensitive information.[354] **Gap Analysis** **Recommendation:** The absence of certain key elements related to this offence in CITO may be remedied using language from Article 4 BC or section 7 HIPCAR. The use of "*without right*" (see above re illicit access) would ensure law enforcement officials, for example, can interfere with data, if appropriate and justified for investigations.

[354] http://www.coe.int/en/web/cybercrime/guidance-notes

Offences		
International Best Practice	**National Legislation**	**Comments**
Section 7 HIPCAR – Illegal Data Interference A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, does any of the following acts: • damages or deteriorates computer data; or • deletes computer data ; or • alters computer data; or • renders computer data meaningless, useless or ineffective; or • obstructs, interrupts or interferes with the lawful use of computer data; or • obstructs, interrupts or interferes with any person in the lawful use of computer data; or • denies access to computer data to any person authorized to access it; commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. **Article 8 CITO** **Offence Against the Integrity of Data** 1. Deliberate unlawful destruction, obliteration, obstruction, modification or concealment of information technology data. 2. The Party may require that, in order to criminalize acts mentioned in paragraph 1, they must cause severe damage.	**Law No.16 of 2017 on Electronic Crimes** **Article 4(3)**	

Offences		
International Best Practice	**National Legislation**	**Comments**
Article 5 BC[355] **System Interference** Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data. **Section 9 HIPCAR – Illegal System Interference** 1. A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification: • hinders or interferes with the functioning of a computer system; or • hinders or interferes with a person who is lawfully using or operating a computer system; commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.	**Law No.16 of 2017 on Electronic Crimes** **Article 4(3)**	**Legal Analysis** CITO does not contain an offence of system interference, it is unclear what wording has been used for the national legislation. Article 11 CITO refers to the *"interfering with the functioning of the operating systems and communication systems, or attempting to disrupt or change them."* And, *"disrupting electronic instruments, programmes and sites.* Albeit this is with the aim of committing *"fraud."* *This offence would prevent malware that interferes with the functioning of a computer by hacktavists without the aim of committing a fraud.* **Gap Analysis** **Recommendation:** The BC language in Article 5 or section 9 HIPCAR are a useful precedent. Also, consider whether the prevention and prosecution of attacks against critical infrastructure needs a separate or aggravated offence (see section 9(2) HIPCAR). This aggravated offence would be relevant when terrorists hinder the functioning of hospital computer systems through a denial of service attack.[356]

[355] no equivalent in CITO

[356] http://www.coe.int/en/web/cybercrime/guidance-notes

Offences		
International Best Practice	**National Legislation**	**Comments**
2. A person who intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification hinders or interferes with a computer system that is exclusively for the use of critical infrastructure operations, or in the case in which such is not exclusively for the use of critical infrastructure operations, but it is used in critical infrastructure operations and such conduct affects that use or impacts the operations of critical infrastructure the punishment shall be imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.		
Article 6 BC **Misuse of Devices** 1. I Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a. the production, sale, procurement for use, import, distribution or otherwise making available of: i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;	**Law No.16 of 2017 on Electronic Crimes** **Article 26**	**Legal Analysis** As above for Illicit Access there is no reference to *"without right"* in CITO Article 9 This offence will enable prosecution for the production, sale, procurement for use, import, distribution of access codes and other computerized data used to commit cybercrimes - for example computer systems may be accessed to facilitate a terrorist attack by interfering with a country's electrical power grid. **Gap Analysis** **Recommendation:** *If* the language in CITO Article 9 is used this does not make it clear if those devices that have a legitimate as well as being put to criminal use (*"dual use"*) are prohibited – this could be remedied by including the BC language of *"**primarily** adapted"* The national law should provide a reasonable excuse so law enforcement can use devices for special investigation techniques – see the language at Article 6.2. BC or section 10(2) HIPCAR as a guide.

Offences		
International Best Practice	National Legislation	Comments
ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b. the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches. 2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3. Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article		

Offences		
International Best Practice	National Legislation	Comments
Article 9 CITO: Offence of Misuse of Information Technology Means 1. The production, sale, purchase, import, distribution or provision of: a. Any tools or programmes designed or adapted for the purpose of committing the offences indicated in Articles 6 to 8. b. The information system password, access code or similar information that allows access to the information system with the aim of using it for any of the offences indicated in Articles 6 to 8. c. The acquisition of any tools or programmes mentioned in the two paragraphs above with the aim of using them to commit any of the offences indicated in Articles 6 to 8 **Section 10 HIPCAR – Illegal Devices** 1. A person commits an offence if the person: a. intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, produces, sells, procures for use, imports, exports, distributes or otherwise makes available: i. a device, including a computer program, that is designed or adapted for the purpose of committing an offence defined by other provisions of Part II of this law; or		

Offences		
International Best Practice	National Legislation	Comments
ii. a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed; with the intent that it be used by any person for the purpose of committing an offence defined by other provisions of Part II of this law; or b. has an item mentioned in subparagraph (i) or (ii) in his or her possession with the intent that it be used by any person for the purpose of committing an offence defined by other provisions of part II of this law commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. 2. This provision shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 is not for the purpose of committing an offence established in accordance with other provisions of Part II of this law, such as for the authorized testing or protection of a computer system. 3. A country may decide not to criminalize illegal devices or limit the criminalization to devices listed in a Schedule.		

Offences		
International Best Practice	**National Legislation**	**Comments**
Article 7 BC **Computer Related Forgery** Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches. **Section 11 HIPCAR – Computer-related Forgery** 1. A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification inputs, alters, deletes, or suppresses computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. 2. If the abovementioned offence is committed by sending out multiple electronic mail messages from or through computer systems, the penalty shall be imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.	**Law No.16 of 2017 on Electronic Crimes** **Article 11**	**Legal Analysis** The language in Article 10 CITO has no reference to any dishonest intent and requires harm to be caused **Gap Analysis** **Recommendation:** The language in BC Article and HIPCAR does not require harm to be caused. BC and HIPCAR only requires that the *"inauthentic data"* data is *"considered"* BC Article 7 or section 11 HIPCAR, therefore, protect against computer related forgery which could include phishing and spear phishing when a received by a victim without harm having been caused. For example, computer data (such as the data used in electronic passports) may be input, altered, deleted, or suppressed with the result that inauthentic data is considered as if it were authentic[357] without any harm being caused. Under CITO this would not be an offence. Also consider section 11(2) HIPCAR (not included in CITO) which provides for the sending of multiple electronic email messages as an aggravated offence.

[357] http://www.coe.int/en/web/cybercrime/guidance-notes

Offences		
International Best Practice	**National Legislation**	**Comments**
Article 10 CITO **Offence of Forgery** The use of information technology means to alter the truth of data in a manner that causes harm, with the intent of using them as true data.		
Article 8 BC **Computer Related Fraud** Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a. any input, alteration, deletion or suppression of computer data, b. any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person. **Article 11 CITO**: **Offence of Fraud** Intentionally and unlawfully causing harm to beneficiaries and users with the aim of committing fraud to illicitly realize interests and benefits to the perpetrator or a third party, through: 1. entering, modifying, obliterating or concealing information and data. 2. interfering with the functioning of the operating systems and communication systems, or attempting to disrupt or change them. 3. disrupting electronic instruments, programmes and sites.	**Law No.16 of 2017 on Electronic Crimes** **Article 14**	**Legal Analysis** The language in Article 11 CITO is vague with no reference to any dishonest intent and requires some form of "*harm*" without defining what this is **Gap Analysis** **Recommendation:** CITO only requires an intent - the language in BC or HIPCAR includes the requirement for a dishonest intent.

Offences		
International Best Practice	**National Legislation**	**Comments**
Section 12 HIPCAR – Computer-related Fraud A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification causes a loss of property to another person by: • any input, alteration, deletion or suppression of computer data; • any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person the penalty shall be imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.		
Article 9 BC **Content related offences (e.g. child pornography)** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a. producing child pornography for the purpose of its distribution through a computer system; b. offering or making available child pornography through a computer system; c. distributing or transmitting child pornography through a computer system; d. procuring child pornography through a computer system for oneself or for another person; e. possessing child pornography in a computer system or on a computer-data storage medium.	**Law No.16 of 2017 on Electronic Crimes** **Article 16**	**Legal Analysis** This is an essential offence in order to protect children from harm by criminalizing the distribution, transmitting, making available, offering, producing and possession of indecent images of children. **Gap Analysis** **Recommendation:** If the language in Article 12 CITO is used there is no definition of child or minor – this should be consistent with extant national legislation. Article 9.3 BC does provide a definition of *"minor"* Further, there is no definition of "outraging public decency" Article 9.2. does provide a definition of *"child pornography"* The CITO offence is committed through *"information technology"* defined in Article 2(1) CITO as, "any material or virtual means or group of interconnected means used to store, sort, arrange, retrieve, process, develop and exchange information according to commands and instructions stored therein. This includes all associated inputs and outputs, by means of wires or wirelessly, in a system or network."

Offences		
International Best Practice	**National Legislation**	**Comments**
2. For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: a. a minor engaged in sexually explicit conduct; b. a person appearing to be a minor engaged in sexually explicit conduct; c. realistic images representing a minor engaged in sexually explicit conduct. 3. For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years. 4. Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c. **Article 12 CITO: Offence of Pornography** 1. The production, display, distribution, provision, publication, purchase, sale, import of pornographic material or material that constitutes outrage of modesty through information technology. 2. The punishment shall be increased for offences related to children and minor pornography. 3. The increase mentioned in paragraph 2 of this Article covers the acquisition of children and minors pornographic material or children and minors material that constitutes outrage of modesty, through information technology or a storage medium for such technology.		As reference is made to "interconnected" this would not include storage mediums as prohibited in Article 9.1.e BC CITO does not cover offences of *"offering" "making available"* or *"procuring for another"* pornographic images of children as prohibited in Article 9.1. BC and section 13 HIPCAR

Offences		
International Best Practice	**National Legislation**	**Comments**
Section 13 HIPCAR – Child Pornography 1. A person who, intentionally, without lawful excuse or justification: • produces child pornography for the purpose of its distribution through a computer system; • offers or makes available child pornography through a computer system; • distributes or transmits child pornography through a computer system; • procures and/or obtain child pornography through a computer system for oneself or for another person; • Possesses child pornography in a computer system or on a computer- data storage medium; or • knowingly obtains access, through information and communication technologies, to child pornography, commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. 2. It is a defense to a charge of an offence under paragraph (1) (b) to (1)(f) if the person establishes that the child pornography was a bona fide law enforcement purpose. 3. A country may not criminalize the conduct described in section 13 (1) (d)- (f).		

Offences		
International Best Practice	**National Legislation**	**Comments**
Article 10 BC **Infringement of copyright** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.	**Law No.16 of 2017 on Electronic Crimes** **Article 8**	**Legal Analysis** Law enforcement internationally utilizes digital copyright offences as additional criminal conduct to investigate and prosecute several forms of cybercrime (which include crimes such as phishing, electronic fraud, electronic forgery, fraudulent websites and data theft/data breaches). One of the underlying offences in many of these cases tends to be infringement of digital copyright. The Sony cyber-attack[358] is only one recent example where offences and powers related to cybercrime, data theft/corporate espionage and copyright infringement came together to complement one another. The absence of any provisions relating to intellectual property would constitute a failure to protect the innovation in the 21st century of the SPCs, businesses and citizens. This may of course be protected in other legislation not reviewed as part of this analysis **Gap Analysis** **Recommendation:** Ensure that there are protections against infringement of copyright that comply with international obligations.

[358] https://en.wikipedia.org/wiki/Sony_Pictures_hack

Offences

International Best Practice	National Legislation	Comments
3. A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article. **Article 17 CITO - Offenses Related to Copyright and Adjacent Rights** Violation of copyright as defined according to the law of the State Party, if the act is committed deliberately and for no personal use, and violation of rights adjacent to the relevant copyright as defined according to the law of the State Party, if the act is committed deliberately and for no personal use.		
Article 11 BC **Aiding and Abetting** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed. 2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.	**Law No.16 of 2017 on Electronic Crimes** **Article 52**	**Legal Analysis** CITO does not have an Article to criminalise those who aid and abet cybercrime. Although Article 19 CITO does include attempts **Gap Analysis** **Recommendation:** Article 19 CITO only refers to attempt and the national legislation should use Article 11 BC as a precedent to ensure those who may have provided assistance or encouraged cybercrimes to take place can be prosecuted.

Offences		
International Best Practice	National Legislation	Comments
Article 19 CITO - Attempt at and Participation in the Commission of Offences 1. Participation in the commission of any of the offences set forth in this chapter with the intention to commit the offence in the law of the State Party. 2. Attempt at the commission the offences set forth in Chapter II of this convention. 3. A State Party may reserve the right to not implement the second paragraph of this Article totally or partly.		
Article 12 BC **Corporate liability** 1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on: a. a power of representation of the legal person; b. an authority to take decisions on behalf of the legal person; c. an authority to exercise control within the legal person. 2. In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.	**Law No.16 of 2017 on Electronic Crimes** **Article 52**	**Legal Analysis** This provision is an essential element so that legal persons (e.g. corporate entities) acting on behalf of natural persons have criminal liability **Gap Analysis** **Recommendation:** Article 20 CITO does not include provision where a corporate entity can be found liable where a relevant natural person had a lack of supervision or control and committed a criminal offence acting under its authority – see Article 12.2. BC

Offences		
International Best Practice	**National Legislation**	**Comments**
3. Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative. 4. uch liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence. **Article 20 CITO: Criminal Responsibility of Natural or Juridical Persons** Every State Party shall commit itself, taking into account its domestic law, to arrange for the penal responsibility of juridical persons for the offences committed by their representatives on their behalf or in their interest, without prejudice to imposing a punishment on the person who committed the offence personally.		
Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems **Article 3[359] – Dissemination of racist and xenophobic material through computer systems** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: distributing, or otherwise making available, racist and xenophobic material to the public through a computer system.	**Law No.16 of 2017 on Electronic Crimes** **Article 24**	**Legal Analysis** If Article 3 of the Additional Protocol has been used this is an appropriate precedent

[359] no equivalent in CITO

Offences		
International Best Practice	**National Legislation**	**Comments**
2. A Party may reserve the right not to attach criminal liability to conduct as defined by paragraph 1 of this article, where the material, as defined in Article 2, paragraph 1, advocates, promotes or incites discrimination that is not associated with hatred or violence, provided that other effective remedies are available. 3. Notwithstanding paragraph 2 of this article, a Party may reserve the right not to apply paragraph 1 to those cases of discrimination for which, due to established principles in its national legal system concerning freedom of expression, it cannot provide for effective remedies as referred to in the said paragraph 2.		
Additional Protocol **Article 4[360] – Racist and xenophobic motivated threat** Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: threatening, through a computer system, with the commission of a serious criminal offence as defined under its domestic law, (i) persons for the reason that they belong to a group, distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors, or (ii) a group of persons which is distinguished by any of these characteristics.	**Law No.16 of 2017 on Electronic Crimes** **Article 24**	**Legal Analysis** If Article 4 of the Additional Protocol has been used this is an appropriate precedent

[360] no equivalent in CITO

Offences		
International Best Practice	**National Legislation**	**Comments**
Additional Protocol **Article 5[361] - Racist and xenophobic motivated insult** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: insulting publicly, through a computer system, (i) persons for the reason that they belong to a group distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors; or (ii) a group of persons which is distinguished by any of these characteristics. 2. A Party may either: a. require that the offence referred to in paragraph 1 of this article has the effect that the person or group of persons referred to in paragraph 1 is exposed to hatred, contempt or ridicule; or b. reserve the right not to apply, in whole or in part, paragraph 1 of this article.	**No equivalent**	**Gap Analysis** **Recommendation:** Use the BC language in Article 5 Additional Protocol as a guide for national legislation

[361] no equivalent in CITO

<table>
<tr><th colspan="3">Offences</th></tr>
<tr><th>International Best Practice</th><th>National Legislation</th><th>Comments</th></tr>
<tr><td><b>Additional Protocol</b>
<b>Article 6[362] - Denial, gross minimisation, approval or justification of genocide or crimes against humanity</b>
1. Each Party shall adopt such legislative measures as may be necessary to establish the following conduct as criminal offences under its domestic law, when committed intentionally and without right: distributing or otherwise making available, through a computer system to the public, material which denies, grossly minimises, approves or justifies acts constituting genocide or crimes against humanity, as defined by international law and recognised as such by final and binding decisions of the International Military Tribunal, established by the London Agreement of 8 August 1945, or of any other international court established by relevant international instruments and whose jurisdiction is recognised by that Party.
2. A Party may either
a. require that the denial or the gross minimisation referred to in paragraph 1 of this article is committed with the intent to incite hatred, discrimination or violence against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors, or otherwise
b. reserve the right not to apply, in whole or in part, paragraph 1 of this article.</td><td><b>Law No.16 of 2017 on Electronic Crimes</b>
<b>Article 25</b></td><td><b>Legal Analysis</b>
<i>If Article 6 of the Additional Protocol has been used this is an appropriate precedent</i></td></tr>
</table>

[362] no equivalent in CITO

Offences		
International Best Practice	**National Legislation**	**Comments**
Additional Offences to Review		
Identity-related Crimes **Section 14 HIPCAR** A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification by using a computer system in any stage of the offence, intentionally transfers, possesses, or uses, without lawful excuse or justification, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a crime, commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.	**Law No.16 of 2017 on Electronic Crimes** **Article 10**	**Legal Analysis** This offence covers the preparation phase of an identity –related crime of dishonesty **Gap Analysis** **Recommendation:** If section 14 HIPCAR has been included this is an appropriate precedent
Disclosure of Details of an Investigation **Section 16 HIPCAR** An Internet service provider who receives an order related to a criminal investigation that explicitly stipulates that confidentiality is to be maintained or such obligation is stated by law and intentionally without lawful excuse or justification or in excess of a lawful excuse or justification discloses: • the fact that an order has been made; or • anything done under the order; or • any data collected or recorded under the order; commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.	**Law No.16 of 2017 on Electronic Crimes** **Article 48**	**Legal Analysis** This offence sanctions data breaches and disclosure of sensitive information that could impact criminal investigations **Gap Analysis** **Recommendation:** If section 16 HIPCAR has been included this is an appropriate precedent

Offences		
International Best Practice	**National Legislation**	**Comments**
Failing to Permit Assistance **Section 17 HIPCAR** 1. A person other than the suspect who intentionally fails without lawful excuse or justification or in excess of a lawful excuse or justification to permit or assist a person based on an order as specified by sections 20 to 22363 commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. 2. A country may decide not to criminalize the failure to permit assistance provided that other effective remedies are available.	**Law No.16 of 2017 on Electronic Crimes** **Article 41**	**Legal Analysis** This offence relates to persons, with specific knowledge of relevant evidence, who refuse to assist. Often law enforcement will be reliant upon such persons to secure evidence in cyber investigations. A separate offence is the failure to provide passwords or access to codes to encrypted devices or data (i.e. *"key to protected information"*) – section 53 of the UK Regulation of Investigatory Powers Act 2000 (RIPA) [364] provides for a criminal offence for persons who fail to comply with a section 49 RIPA Notice to disclose the *"key"* **Gap Analysis** **Recommendation:** If section 17 HIPCAR has been included this is an appropriate precedent A separate offence is recommended for the failure to provide passwords or access to codes to encrypted devices or data (i.e. *"key to protected information"*) – section 53 of the UK Regulation of Investigatory Powers Act 2000 (RIPA) provides for a criminal offence for persons who fail to comply with a section 49 RIPA Notice to disclose the *"key"*
Cyber Stalking **Section 18 HIPCAR** A person, who without lawful excuse or justification or in excess of a lawful excuse or justification initiates any electronic communication, with the intent to coerce, intimidate, harass, or cause substantial emotional distress to a person, using a computer system to support severe, repeated, and hostile behavior, commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.	**Law No.16 of 2017 on Electronic Crimes** **Article 15**	**Legal Analysis** This offence criminalizes those who harass persons online– some jurisdictions may have non-computer related harassment offences – but this offence is recommended for those crimes committed online. **Gap Analysis** **Recommendation:** *If* section 18 HIPCAR has been included this is an appropriate precedent

[363] Search and seizure, assistance and production orders

[364] http://www.legislation.gov.uk/ukpga/2000/23/section/53

Offences		
International Best Practice	National Legislation	Comments
Grooming Children Online **Dutch Criminal Code 248e** The person who proposes to arrange a meeting, by means of an automated work or by making use of a communication service, to a person of whom he knows, or should reasonably assume, that such person has not yet reached the age of sixteen, with the intention of committing indecent acts with this person or of creating an image of a sexual act in which this person is involved, will be punished with a term of imprisonment of at most two years or a fine of the fourth category, if he undertakes any action intended to realise that meeting. **Canadian Criminal Code** **Section 172.1** 1. Every person commits an offence who, by a means of telecommunication, communicates with a. a person who is, or who the accused believes is, under the age of 18 years, for the purpose of facilitating the commission of an offence under subsection 153(1), section 155, 163.1, 170 or 171 or subsection 212(1), (2), (2.1) or (4) with respect to that person; b. a person who is, or who the accused believes is, under the age of 16 years, for the purpose of facilitating the commission of an offence under section 151 or 152, subsection 160(3) or 173(2) or section 271, 272, 273 or 280 with respect to that person; or	**Law No.16 of 2017 on Electronic Crimes** **Articles 16(3), (4) and 56**	**Legal Analysis** To prove the Dutch offence a meeting for sexual purposes is required with supporting evidence of online chat history with sexual intent; request for a meeting with evidence this was planned (i.e. date and place). The purpose of the Canadian law is to prevent grooming by predatory adults of children online. This offence does not require the sexual offence to have occurred. This means the accused does not need to have actually gone to meet the victim in person. The offence is committed before any actions are taken to commit the substantive offence. **Gap Analysis** **Recommendation:** If the national legislation prohibits grooming, without a meeting having necessarily taken place, this is appropriate.

Offences		
International Best Practice	**National Legislation**	**Comments**
c. a person who is, or who the accused believes is, under the age of 14 years, for the purpose of facilitating the commission of an offence under section 281 with respect to that person. Punishment 2. Every person who commits an offence under subsection (1) is guilty of a. is guilty of an indictable offence and is liable to imprisonment for a term of not more than 10 years and to a minimum punishment of imprisonment for a term of one year; or b. is guilty of an offence punishable on summary conviction and is liable to imprisonment for a term of not more than 18 months and to a minimum punishment of imprisonment for a term of 90 days. Presumption re age 3. Evidence that the person referred to in paragraph (1)(a), (b) or (c) was represented to the accused as being under the age of eighteen years, sixteen years or fourteen years, as the case may be, is, in the absence of evidence to the contrary, proof that the accused believed that the person was under that age. No defence 4. It is not a defence to a charge under paragraph (1)(a), (b) or (c) that the accused believed that the person referred to in that paragraph was at least eighteen years of age, sixteen years or fourteen years of age, as the case may be, unless the accused took reasonable steps to ascertain the age of the person.		

Procedure		
International Best Practice	National Legislation	Comments
Article 26 CITO - Inspecting Stored Information 1. Every State Party shall commit itself to adopting the procedures necessary to enable its competent authorities to inspect or access: a. an information technology or part thereof and the information stored therein or thereon. b. the storage environment or medium in or on which the information may be stored. 2. Every State Party shall commit itself to adopting the procedures necessary to enable the competent authorities to inspect or access a specific information technology or part thereof in conformity with paragraph 1(a) if it is believed that the required information is stored in another information technology or in part thereof in its territory and such information is legally accessible or available in the first technology, the scope of inspection may be extended and the other technology accessed. **Article 27 CITO - Seizure of Stored Information** 1. Every State Party shall commit itself to adopting the procedures necessary to enable the competent authorities to seize and safeguard information technology information accessed according to Article 26, paragraph 1, of this Convention. These procedures include the authority to:	**Decree Law No. 20 of 2015 on Combating Money Laundering and the Financing of Terrorism** **Article 33** Powers of the Attorney General: The Attorney General may, on the basis of a decision of the competent court....Access to computer systems and networks and main computers **Law No.16 of 2017 on Electronic Crimes** **Article 33** **Article 34:** 1. The Public Prosecution shall have access to devices, tools, means, data, electronic information, traffic data, data relating to the traffic of the Communications or its users, or content information related to electronic crime. 2. The Public Prosecution has the right to authorize and strictly maintain the entire information system or part of it or any means of information technology that would help to uncover the truth. 3. If the seizing of information system is not necessary or cannot be performed, the data or information related to the crime and the data that is believed to be read and understood will be copied on one of the means of information technology.	**Legal Analysis** *This is the most essential investigatory power and should refer to gaining access than search. In the BC Explanatory Report, "Search" means to seek, read, inspect or review data. It includes the notion of searching for data and searching of (examining) data. The word "access" has a neutral meaning and reflects more accurately computer terminology – this is also included in Articles 26 and 27 CITO.*[365] Article 33 Decree Law No. 20 of 2015 relates to the access but is only available for money laundering and the financing of terrorism. Article 33 No. 16 of 2017 will be more wide-ranging and applies to the cybercrime offences it criminalises. Article 34(1) confirms access to computers and data relevant to crimes in law No. 16. Article 34(3) enables copying of the relevant data if not seized. Article 34(4) prevents access if the data cannot be seized and Article 34(5) requires integrity of the seized data is maintained. These provisions are consistent with CITO

[365] Paragraph 191 page 33 Explanatory Report BC

Procedure		
International Best Practice	**National Legislation**	**Comments**
a. a.seize and safeguard the information technology or part thereof or the storage medium for the information technology information. b. b.make a copy the information technology information and keep it. c. c.maintain the integrity of the stored information technology information. d. d.remove such accessed information from the information technology or prevent its access. 2. Every State Party shall commit itself to adopting the procedures necessary to enable the competent authorities to order any person who is acquainted with the functioning of the information technology or the procedures applied to protect the information technology to give the information necessary to complete the procedures mentioned in paragraphs 2 and 3 of Article 26 of this Convention.	4. If it is impossible to carry out the seizure or to effectively detain it, in order to preserve the evidence of the crime, all appropriate means shall be used to prevent access to and access to data stored in the information system. 5. The necessary precautions are to be taken to maintain the integrity of the seized seizure, including technical means to protect its content. 6. A recorded report shall be kept in the presence of the accused or of those found to have the seized seizure. The seized seizure shall be kept in accordance with the case in a sealed envelope or envelope, with a paper stating the date and time of the reservation and the number of records and case.	

Procedure		
International Best Practice	**National Legislation**	**Comments**
Article 16 BC **Expedited preservation of stored computer data** 1. Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2. Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.	**Law No.16 of 2017 on Electronic Crimes** **Article 34**	**Legal Analysis** This procedural power is important to ensure that data which is vulnerable to deletion or loss is preserved **Gap Analysis** **Recommendation:** This expedited power to retain BSI, traffic data, transactional and stored content is essential as part of cybercrime investigations to ensure the evidence is available for search, access, seizure and review. The national legislation will require sufficient definitions of "subscriber information or BSI",[366] *"traffic data"*[367] and *"Communication Service Provider"*[368] to ensure it can be preserved. Consideration should be given the length of preservation that is reasonable in the circumstances and allowing for an application to extend in exigent circumstances – BC and CITO have 90 days and HIPCAR 7 days. From experience 90 days is too few in a cyber investigation and the figure should be nearer 180 days and then subject to extension.

[366] See definition in Glossary above or Article 2(9) CITO: "*Any information that the service provider has concerning the subscribers to the service, except for information through which the following can be known: a. the type of communication service used, the technical requirements and the period of service. b. the identity of the subscriber, his postal or geographic address or phone number and the payment information available by virtue of the service agreement or arrangement. c. any other information on the installation site of the communication equipment by virtue of the service agreement.*"

[367] See Article 1.d BC: "*any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service*" **or** section 3(18) HIPCAR: "*Traffic data means computer data that: a. relates to a communication by means of a computer system; and b. is generated by a computer system that is part of the chain of communication ; and c. shows the communication's origin, destination, route, time date, size, duration or the type of underlying services.*"

[368] See Article 1.c. BC: "*i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii any other entity that processes or stores computer data on behalf of such communication service or users of such service*" **or** Article 2(2) CITO: "*any natural or juridical person, common or private, who provides subscribers with the services needed to communicate through information technology, or who processes or stores information on behalf of the communication service or its users.*"

Procedure		
International Best Practice	National Legislation	Comments
3. Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. 4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15. **Section 23 HIPCAR – Expedited Preservation** If a [law enforcement] [police] officer is satisfied that there are grounds to believe that computer data that is reasonably required for the purposes of a criminal investigation is particularly vulnerable to loss or modification, the [law enforcement] [police] officer may, by written notice given to a person in control of the computer data, require the person to ensure that the data specified in the notice be preserved for a period of up to seven (7) days as specified in the notice. The period may be extended beyond seven (7) days if, on an ex parte application, a [judge] [magistrate] authorizes an extension for a further specified period of time. **Article 23 CITO - Expeditious Custody of Data Stored in Information Technology** 1. Every State Party shall adopt the procedures necessary to enable the competent authorities to issue orders or obtain the expeditious custody of information, including information for tracking users, that was stored on an information technology, especially if it is believed that such information could be lost or amended.		

Procedure		
International Best Practice	**National Legislation**	**Comments**
2. Every State Party shall commit itself to adopting the procedures necessary as regards paragraph 1, by means of issuing an order to a person to preserve the information technology information in his possession or under his control, in order to require him to preserve and maintain the integrity of such information for a maximum period of 90 days that may be renewed, in order to allow the competent authorities to search and investigate 3. Every State Party shall commit itself to adopting the procedures necessary to require the person responsible for safeguarding the information technology to maintain the procedures secrecy throughout the legal period stated in the domestic law.		
Article 24 CITO - Expeditious Custody and Partial Disclosure of Users Tracking Information Every State Party shall commit itself to adopting the procedures necessary as regards users tracking information in order to: 1. ensure expeditious custody of users tracking information, regardless of whether such communication is transmitted by one or more service providers. 2. ensure that a sufficient amount of users tracking information is disclosed to the competent authorities of the State Party or to a person appointed by these authorities to allow the State Party to determine the service providers and the transmission path of the communications.	**Law No.16 of 2017 on Electronic Crimes** **Article 34**	**Legal Analysis** This procedural power is especially important to ensure that CSPs provide IP addresses that could locate either the perpetrator of a cybercrime CITO does not have a definition of "tracking information" – this would be different to traffic data as the latter would include the communication's origin, destination, route, time, date, size, duration, or type of underlying service (see Article 1.d. BC or section 3(18) HIPCAR) **Gap Analysis** **Recommendation:** This expedited power, alongside disclosure of traffic data, should include definitions of *"traffic data"* and *"Communication Service Provider"*[369]

[369] See definitions above

Procedure		
International Best Practice	National Legislation	Comments
Article 25 CITO - Order to Submit Information Every State Party shall commit itself to adopting the procedures necessary to enable the competent authorities to issue orders to: 1. Any person in its territory to submit certain information in his possession which is stored on information technology or a medium for storing information. 2. Any service provider offering his services in the territory of the State Party to submit user's information related to that service which is in the possession of the service provider or under his control.	**Law No.16 of 2017 on Electronic Crimes** **Article 32** **Production Order**	**Legal Analysis** This is an essential provision for an effective cybercrime investigation and its absence will impact upon prosecutions and international cooperation. **Gap Analysis** **Recommendation:** This essential power is necessary to ensure CSPs in PA provide BSI, traffic data and stored content data. This will also require definitions of *"subscriber information or BSI"*, *"traffic data"* and *"Communication Service Provider"*.[370] Article 25 CITO uses definitions including *"information technology"*,[371] *"service provider"*[372] and *"data"*[373] – it is still advisable to have definitions for *"subscriber information or BSI"* and *"traffic data"* as they will be different types of evidence that can be produced from CSPs. Further, this power will require individuals and others (such as corporate entities, financial institutions and other organisations) who hold data to produce it to law enforcement authorities.
Article 29 CITO - Interception of Content Information 1. Every State Party shall commit itself to adopting the legislative procedures necessary as regards a series of offences set forth in the domestic law, in order to enable the competent authorities to: a. gather or register through technical means in the territory of this State Party, or	**Decree Law No. 20 of 2015 on Combating Money Laundering and the Financing of Terrorism** **Article 33** The Attorney General may, upon a decision of the competent court, 1. Control of bank accounts and other similar accounts. 2. Access to computer systems and networks and main computers	**Legal Analysis** This power is essential for national legislation to compel CSPs cooperation to collect or record content data in real-time in PA. Article 33 Decree Law No. 20 of 2015 relates only for money laundering and financing of terrorism investigations. Article 35 of Law No. 16 of 2017 will be more wide-ranging and applies to the cybercrime offences it criminalizes.

[370] ibid

[371] Article 2(1) CITO: *"any material or virtual means or group of interconnected means used to store, sort, arrange, retrieve, process, develop and exchange information according to commands and instructions stored therein. This includes all associated inputs and outputs, by means of wires or wirelessly, in a system or network."*

[372] Article 2(2) CITO: *"any natural or juridical person, common or private, who provides subscribers with the services needed to communicate through information technology, or who processes or stores information on behalf of the communication service or its users."*

[373] Article 2(3) CITO: *"all that may be stored, processed, generated and transferred by means of information technology, such as numbers, letters, symbols, etc…"* - Article 1.b. BC also includes a program suitable to cause a computer system to perform a function

Procedure		
International Best Practice	National Legislation	Comments
b. cooperate with and help the competent authorities to expeditiously gather and register content information of the relevant communications in its territory and which are transmitted by means of the information technology. 2. If, because of the domestic legal system, the State Party is unable to adopt the procedures set forth in paragraph 1(a), it may adopt other procedures in the form necessary to ensure the expeditious gathering and registration of content information corresponding to the relevant communications in its territory using the technical means in that territory. 3. Every State Party shall commit itself to adopting the procedures necessary to require the service provider to maintain the secrecy of any information when exercising the authority set forth in this Article.	3. Subject to surveillance or tracking of communications. 4. Audio and visual recording or portraying acts, behavior or conversations. 5. Intercepting and booking correspondence. **Law No.16 of 2017 on Electronic Crimes** **Article 35(2)** The Public Prosecution may order the immediate collection and supply of any data including traffic, electronic information, traffic data or content information that it deems necessary for the benefit of the investigations, using the appropriate technical means and, where appropriate, using the service providers according to the type of service it provides.	
Article 28 CITO **Expeditious gathering of users tracking information**	**Law No.16 of 2017 on Electronic Crimes** **Article 35(2)** The Public Prosecution may order the immediate collection and supply of any data **including traffic, electronic information, traffic data** or content information that it deems necessary for the benefit of the investigations, using the appropriate technical means and, where appropriate, using the service providers according to the type of service it provides.	**Legal Analysis** Article 35(2) has the same threshold for content information - namely collection of traffic data if necessary for the investigation. **Gap Analysis** **Recommendations:** Consideration could be given to a different threshold. There may be situations where a higher legal threshold to secure content is not made out by an applicant – but a lower threshold to secure traffic can be. For this reason, there could be a distinction between real-time collection of stored content and traffic data.

Procedure

International Best Practice	National Legislation	Comments
		Data retention obligations[374] Such a power can allow law enforcement to 1. Trace and identify the source of a communication 2. Identify the destination of a communication; 3. Identify the date, time and duration of a communication; and 4. Identify the type of communication Unable to identify if PA does have such an obligation[375]

International Cooperation

International Best Practice	National Legislation	Comments
Article 30 CITO - Competence 1. Every State Party shall commit itself to adopting the procedures necessary to extend its competence to any of the offences set forth in Chapter II of this Convention, if the offence is committed, partly or totally, or was realized: a. in the territory of the State Party b. on board a ship raising the flag of the State Party. c. on board a plane registered under the law of the State Party. d. by a national of the State Party if the offence is punishable according to the domestic law in the location where it was committed, or if it was committed outside the jurisdiction of any State.	**Law No.16 of 2017 on Electronic Crimes** **Article 2**	**Legal Analysis** Article will ensure a clearly defined scope for cybercrime offences, that are international in nature. **Gap Analysis** **Recommendation:** National legislation ensures jurisdiction is defined. If there is a conflict between jurisdictions consideration should be given to guidelines on determining the appropriate jurisdiction to try an offence – see the Eurojust Guidelines for Deciding which Jurisdiction should Prosecute (revised 2016)[376]

[374] In 2006 the EU issued its Data Retention Directive - EU Member States had to store electronic telecommunications data for at least six months and at most 24 months for investigating, detecting and prosecuting serious crime. In 2014, the Court of Justice of the EU invalidated the Data Retention Directive, holding that it provided insufficient safeguards against interferences with the rights to privacy and data protection. In the absence of a valid EU Data Retention Directive, Member States may still provide for a data retention scheme – for national schemes see: http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention

[375] ICMEC Global Review page 30

[376] http://www.eurojust.europa.eu/Practitioners/operational/Documents/Operational-Guidelines-for-Deciding.pdf

International Cooperation		
International Best Practice	National Legislation	Comments
e. if the offence affects an overriding interest of the State. 2. Every State Party shall commit itself to adopting the procedures necessary to extend the competence covering the offences set forth in Article 31, paragraph 1, of this Convention in the cases in which the alleged offender is present in the territory of that State Party and shall not extradite him to another Party according to his nationality following the extradition request. 3. If more than one State Party claim to have jurisdiction over an offence set forth in this Convention, priority shall be accorded to the request of the State whose security or interests were disrupted by the offence, followed by the State in whose territory the offence was committed, and then by the State of which the wanted person is a national. In case of similar circumstances, priority shall be accorded to the first State that requests the extradition.		

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
Article 43 CITO **Specialized Body**[377] 1. Every State Party shall guarantee, according to the basic principles of its legal system, the presence of a specialized body dedicated 24 hours a day to ensure the provision of prompt assistance for the purposes of investigation, procedures related to information technology offences or gather evidence in electronic form regarding a specific offence. Such assistance shall involve facilitating or implementing: a. provision of technical advice. b. safeguarding information based on Articles 37 and 38. c. collecting evidence, provide legal information and locate suspects. 2. a. In all State Parties, such a body shall be able to communicate promptly with the corresponding body in any other State Party b. If the said body, designated by a State Party, is not part of the authorities of that State Party responsible for international bilateral assistance, that body shall ensure its ability to promptly coordinate with those authorities. 3. Every State Party shall ensure the availability of capable human resources to facilitate the work of the above mentioned body.	**No equivalent**	**Legal Analysis** This is an essential mechanism for an effective cybercrime investigative capability. **Gap Analysis** **Recommendation:** This should not require legislation to implement and subject to resources should be established as a priority. Contact details should be shared for the nominated single point of contact (SPOC) nationally, central authorities internationally and INTERPOL. Consideration should also be given to drafting a Memorandum of Understanding with national agencies so that the SPOC has authority to undertake the actions required as part of an international cybercrime investigation applying national laws and treaties. This MOU will include both incoming and outgoing requests and ensure an efficient and effective process.

[377] Article 35 BC

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
Article 34 CITO - Procedures for Cooperation and Mutual Assistance Requests 1. The provisions of paragraphs 2-9 of this Article shall apply in case no cooperation and mutual assistance treaty or convention exists on the basis of the applicable legislation between the State Parties requesting assistance and those from which assistance is requested. If such a treaty or convention exists, the mentioned paragraphs shall not apply, unless the concerned parties agree to apply them in full or in part. 2. a. Every State Party shall designate a central authority responsible for sending and responding to mutual assistance requests and for their implementation and referral to the relevant authorities for implementation. b. Central authorities shall communicate directly among themselves. c. Every State Party shall, at the time of signature or deposit of the instrument of ratification, acceptance or agreement, contact the General Secretariat of the Council of Arab Interior Ministers and the Technical Secretariat of the Arab Justice Ministers and communicate to them the names and addresses of the authorities specifically designated for the purposes of this paragraph.	**Law No.16 of 2017 on Electronic Crimes** **Articles 43 and 44**	**Legal Analysis** Articles 32 and 34 CITO ensure that it can be used as an instrument to facilitate MLA and the national law now provides for expedited preservation of stored computer data, expedited preservation and partial disclosure of traffic data and disclosure of stored data and traffic data, interception of content data, real-time collection of traffic data, production orders, search and seizure to CITO states. Equally, through the principle of reciprocity, PA can execute requests from those States who are signatories to the BC and others who have the same procedural measures.

International Cooperation		
International Best Practice	National Legislation	Comments
d. The General Secretariat of the Council of Arab Interior Ministers and the Technical Secretariat of the Arab Justice Ministers shall establish and update a registry of concerned central authorities appointed by the State Parties. Every State Party shall insure that the registry's details are correct at all times 3. Mutual assistance requests in this Article shall be implemented according to procedures specified by the requesting State Party, except in the case of non conformity with the law of the State Party from which assistance is requested. 4. The State Party from which assistance is requested may postpone taking action on the request if such action shall affect criminal investigations conducted by its authorities. 5. Prior to refusing or postponing assistance, the State Party from which assistance is requested shall decide, after consulting with the requesting State Party, whether the request shall be partially fulfilled or be subject to whatever conditions it may deem necessary. 6. The State Party from which assistance is requested shall commit itself to inform the requesting State Party of the result of the implementation of the request. If the request is refused or postponed, the reasons of such refusal or postponement shall be given. The State Party from which assistance is requested shall inform the requesting State Party of the reasons that prevent the complete fulfilment of the request or the reasons for its considerable postponement.		

International Cooperation		
International Best Practice	National Legislation	Comments
7. The State Party requesting assistance may request the State Party from which assistance is requested to maintain the confidentiality of the nature and content of any request covered by this chapter, except in as far as necessary to implement the request. If the State Party from which assistance is requested cannot abide by this request concerning confidentiality, it shall so inform the requesting State Party which will then decide about the possibility of implementing the request. 8. a. In case of emergency, mutual assistance requests may be sent directly to the judicial authorities in the State Party from which assistance is requested from their counterparts in the requesting State Party. In such case, a copy shall be sent concurrently from the central authority in the requesting State Party to its counterpart in the State Party from which assistance is requested. b. Communications can be made and requests submitted pursuant to this paragraph through INTERPOL. c. Whenever, according to paragraph a, a request is submitted to an authority, but that authority is not competent to deal with that request, it shall refer the request to the competent authority and directly inform the requesting State Party accordingly.		

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
d. Communications and requests carried out according to this paragraph and not concerning compulsory procedures may be transmitted directly by the competent authorities in the requesting State Party to their counterpart in the State Party from which assistance is requested. e. very State Party may, at the time of signature, ratification, acceptance or adoption, inform the General Secretariat of the Council of Arab Interior Ministers and the Technical Secretariat of the Arab Justice Ministers that requests according to this paragraph must be submitted to the central authority for reasons of efficiency.		

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
Article 33 CITO - Circumstantial Information 1. A State Party may – within the confines of its domestic law – and without prior request, give another State information it obtained through its investigations if it considers that the disclosure of such information could help the receiving State Party in investigating offences set forth in this convention or could lead to a request for cooperation from that State Party. 2. Before giving such information, the State Party providing it may request that the confidentiality of the information be kept; if the receiving State Party cannot abide by this request, it shall so inform the State Party providing the information which will then decide about the possibility of providing the information. If the receiving State Party accepts the information on condition of confidentiality, the information shall remain between the two sides.	**Law No.16 of 2017 on Electronic Crimes** **Article 43**	**Legal Analysis** This is an important procedure to enable a state privy to information that will assist another state to prevent a cybercrime or to investigate it. PA now has no domestic legal basis to share such information **Gap Analysis** **Recommendation:** Guarantees should be considered about use of the spontaneously provided information in evidence or disclosure of sensitive information to a third party (including another state).[378]
Article 40 CITO - Access to Information Technology Information Across Borders A State Party may, without obtaining an authorization from another State Party: 1. Access information technology information available to the public (open source), regardless of the geographical location of the information.	**Law No.16 of 2017 on Electronic Crimes** **Article 40**	**Legal Analysis** This procedural power enables a state to secure content stored in another state in limited circumstances. Article 40 CITO is an exception to the principle of territoriality and permits unilateral trans-border access without the need for mutual legal assistance where there is consent of the user or the information is publicly available.

[378] See Article 33(2) CITO

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
2. Access or receive – through information technology in its territory – information technology information found in the other State Party, provided it has obtained the voluntary and legal agreement of the person having the legal authority to disclose information to that State Party by means of the said information technology. **Section 27 HIPCAR – Forensic Software** 1. If a [judge] [magistrate] is satisfied on the basis of [information on oath] [affidavit] that in an investigation concerning an offence listed in paragraph 7 herein below there are reasonable grounds to believe that essential evidence cannot be collected by applying other instruments listed in Part IV but is reasonably required for the purposes of a criminal investigation, the [judge] [magistrate] [may] [shall] on application authorize a [law enforcement] [police] officer to utilize a remote forensic software with the specific task required for the investigation and install it on the suspect's computer system in order to collect the relevant evidence. The application needs to contain the following information: • suspect of the offence, if possible with name and address; and • description of the targeted computer system; and • description of the intended measure, extent and duration of the utilization; and		Examples of use of this procedural power include: A person's e-mail may be stored in another country by a service provider, or a person may intentionally store data in another State. These persons may retrieve the data and, provided that they have the lawful authority, they may voluntarily disclose the data to law enforcement officials or permit such officials to access the data[379] Or A suspected terrorist is lawfully arrested while his/her mailbox – possibly with evidence of a crime – is open on his/her tablet, smartphone or other device. If the suspect voluntarily consents that the police access the account and if the police are sure that the data of the mailbox is located in another state, police may access the data. **Gap Analysis** **Recommendation:** This restricted power to unilaterally secure evidence is now included in legislation with safeguards to ensure the consent is lawfully obtained from the user.[380] Article 40 does not provide for the Requested State to consent. Section 27 HIPCAR provides a number of restrictions that requires the evidence cannot be obtained by other means, a judicial order is required, can only apply to certain offences and is for a restricted period (3 months). Consideration should also be given to consent of the other state where the forensic software may intrude.

[379] Paragraph 294, page 52 BC Explanatory Report

[380] Consideration should be given to situations such as the non-availability of a user (e.g. death) and if consent can be obtained in another state

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
• reasons for the necessity of the utilization. 2. Within such investigation it is necessary to ensure that modifications to the computer system of the suspect are limited to those essential for the investigation and that any changes if possible can be undone after the end of the investigation. During the investigation, it is necessary to log • the technical mean used and time and date of the application; and • the identification of the computer system and details of the modifications undertaken within the investigation; • any information obtained. Information obtained by the use of such software needs to be protected against any modification, unauthorized deletion and unauthorized access. 3. The duration of authorization in section 27 (1) is limited to [3 months]. If the conditions of the authorization is no longer met, the action taken are to stop immediately. 4. The authorization to install the software includes remotely accessing the suspects computer system. 5. If the installation process requires physical access to a place the requirements of section 20 need to be fulfilled. 6. If necessary a [law enforcement] [police] officer may pursuant to the order of court granted in (1) above request that the court order an internet service provider to support the installation process. 7. [List of offences]. 8. A country may decide not to implement section 27.		

Tunisia

It should be noted that although Tunisia does not yet have legislation on cybercrime a bill is being prepared. Tunisia has acceded to Convention No. 108 of the Council of Europe for Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and its additional protocol No 181 for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and trans-border data flows.[381] These ratified Conventions occupy the second place in the pyramid of legal texts in Tunisia just after the constitution and before the laws and decrees.

Offences		
Budapest Convention on Cybercrime ('BC')	**National Legislation**	**Comments**
Article 2 BC – Illegal access[382] Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system. **Article 6 CITO – Illicit Access** 1. Illicit access to, presence in or contact with part or all of the information technology, or the perpetuation thereof. 2. The punishment shall be increased if this access, presence, contact or perpetuation leads to: a. the obliteration, modification, distortion, duplication, removal or destruction of saved data, electronic instruments and systems and communication networks, and damages to the users and beneficiaries.	**Penal Code** **Article 199 bis** Anyone who, fraudulently, has acceded or will have maintained himself in all or part of an automated data processing system,	**Legal Analysis** The national provision includes reference to *"fraudulently"* this would suggest that the perpetrator has accessed the data dishonestly – whereas the BC refers to *"without right"* on the basis access is unauthorized. The BC refers to a "dishonest intent" but this relates to securing data rather than the act of gaining illegal access. At present this national offence can only be committed where the perpetrator dishonestly represents the purpose for accessing. It is unclear without a definition of *"fraudulently"* if this requires an overt action or if every illegal access is deemed to be fraudulent. It is for this reason that a definition of *"fraudulent"* is required. The offence also refers to a *"automated data processing system"* without a definition. It is unclear if this relates to a "computer system" (i.e. means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data – Article 1 BC) or "computerised data" (i.e. any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function – Article 1 BC) Article 6 CITO refers to *"illicit access to, presence in or contact with"* without defining what these acts mean – therefore, BC and HIPCAR are to be preferred.

[381] Organic Law 2017-42 of 30 May 2017 approving the accession of the Republic of Tunisia to Convention No. 108 of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data and its Additional Protocol No. 181 concerning supervisory authorities and trans-border data flows

[382] Article 29(1) AUC

Offences		
Budapest Convention on Cybercrime ('BC')	**National Legislation**	**Comments**
b. the acquirement of secret government information. **Section 4 HIPCAR – Illegal Access** 1. A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, accesses the whole or any part of a computer system commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. 2. A country may decide not to criminalize the mere unauthorized access provided that other effective remedies are available. Furthermore, a country may require that the offence be committed by infringing security measures or with the intent of obtaining computer data or other dishonest intent. **Section 5 HIPCAR – Illegal Remaining** 1. A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, remains logged in a computer system or part of a computer system or continues to use a computer system commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. 2. A country may decide not to criminalize the mere unauthorized remaining provided that other effective remedies are available. Alternatively, a country may require that the offence be committed by infringing security measures or with the intent of obtaining computer data or other dishonest intent.		**Recommendation:** The national legislation could incorporate relevant language from the BC and/or HIPCAR to include definitions of a computer system and the inclusion of programs within the definition of data as some data includes programs and other data does not. Further, to be consistent with the BC/HIPCAR refer to access *"without right"* rather than fraudulently. Consideration should be given to an aggravated offence if illegal access is gained to a critical infrastructure computer system or data

Offences		
Budapest Convention on Cybercrime ('BC')	**National Legislation**	**Comments**
Article 3 BC[383] - **Illegal Interception** Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system. **Section 6 HIPCAR – Illegal Interception** 1. A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, intercepts by technical means: a. any non-public transmission to, from or within a computer system; or b. electromagnetic emissions from a computer system commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.	**No equivalent**	**Legal Analysis** This offence is essential to prosecute non-public transmissions of computer data to, from, or within a computer system that may be illegally intercepted to obtain information about a person's location (e.g. to target that person).[384] Tunisia has acceded to Convention No. 108 of the Council of Europe for the Protection of Individuals, with regard to the automatic processing of personal data and its Additional Protocol No 181 concerning supervisory authorities and trans-border data flows.385 This legislation will protect individuals against abuses which may accompany the collection and processing of personal data as enshrined in the Convention. Although not explicit, this would include data obtained through illegal interception. In addition, the Convention provides guarantees in relation to the collection and processing of personal data, and prohibits the processing of *"sensitive"* data on a person's race, politics, health, religion, sexual life, criminal record, etc., in the absence of proper legal safeguards. The Convention also enshrines the individual's right to know that information is stored on him or her and, if necessary, to have it corrected. Restriction on the rights laid down in the Convention are only possible when overriding interests (e.g. State security, defence, etc.) are at stake. This would mean that if there is legal interception[386] the data would be lawfully collected and processed. The Convention also imposes some restrictions on trans-border flows of personal data to States where legal regulation does not provide equivalent protection.[387]

[383] Article 29(2) AUC

[384] http://www.coe.int/en/web/cybercrime/guidance-notes

[385] ibid

[386] Organic Law No. 2015-26 of 7 August 2015 relating to the fight against terrorism and the repression of the money bleaching Article 54 or Organic Law No. 2016-61 of 3 August 2016 related to the Prevention and Combating of Trafficking in Persons Article 32

[387] Summary of Convention No. 108 at: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

Offences

Budapest Convention on Cybercrime ('BC')	National Legislation	Comments
2. A country may require that the offence be committed with a dishonest intent, or in relation to a computer system that is connected to another computer system, or by circumventing protection measures implemented to prevent access to the content of non-public transmission. **Article 7 CITO** **Illicit Interception** The deliberate unlawful interception of the movement of data by any technical means, and the disruption of transmission or reception of information technology data.		**Gap Analysis** **Recommendation:** Use the BC language in Article 3, HIPCAR section 6 as a guide - the language in Article 7 CITO is appropriate – albeit there is no definition of "*information technology data*"
Article 4 BC[388] **Data Interference** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right. 2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm. **Section 7 HIPCAR – Illegal Data Interference** A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, does any of the following acts: • damages or deteriorates computer data; or • deletes computer data ; or • alters computer data; or	**Penal Code** **Article 199 bis** *:* The penalty is increased to two years' imprisonment and the fine to two thousand dinars where it results, even without intent, when there is modification or destruction of the exploitation of the existing data in the system indicated….. Anyone who has fraudulently introduced data into an automated processing system that is liable to alter the data contained in the program or the manner in which it is processed or transmitted is punished by imprisonment for five years and a fine of five thousand dinars. The penalty shall be doubled when the act referred to above is committed by a person in the exercise of his functions.	**Legal Analysis** The use of *"fraudulently"* is inconsistent (in fact in conflict with) the standard of the BC 4.1 "…when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right" which does not require fraud to be proved. This means that conduct which constitutes an offence of data interference under the BC's 4.1 would not be criminalized under Article 199 bis. This Article does not include element of suppression of computer data **Gap Analysis** **Recommendation:** Use Article 4 BC or section 7 HIPCAR as a guide to amend/ replace national legislation

[388] Article 29(1)(e-f) AUC

Offences		
Budapest Convention on Cybercrime ('BC')	**National Legislation**	**Comments**
- renders computer data meaningless, useless or ineffective; or - obstructs, interrupts or interferes with the lawful use of computer data; or - obstructs, interrupts or interferes with any person in the lawful use of computer data; or - denies access to computer data to any person authorized to access it; commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. **Article 8 CITO** **Offence Against the Integrity of Data** 1. Deliberate unlawful destruction, obliteration, obstruction, modification or concealment of information technology data. 2. The Party may require that, in order to criminalize acts mentioned in paragraph 1, they must cause severe damage.		
Article 5 BC[389] **System Interference** Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.	**Penal Code** **Article 199 bis** Anyone who intentionally alters or destroys the operation of automated processing	**Legal Analysis** This offence would prevent malware that interferes with the functioning of a computer – for example computer worms - a subgroup of malware (like computer viruses). They are self-replicating computer programs that harm the network by initiating multiple data-transfer processes. They can influence computer systems by hindering the smooth running of the computer system, using system resources to replicate themselves over the Internet or generating network traffic that can close down availability of certain services (such as websites)

[389] Article 29(1)(d) AUC no equivalent in CITO

Offences		
Budapest Convention on Cybercrime ('BC')	**National Legislation**	**Comments**
Section 9 HIPCAR – Illegal System Interference 1. A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification: • hinders or interferes with the functioning of a computer system; or • hinders or interferes with a person who is lawfully using or operating a computer system; commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. 2. A person who intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification hinders or interferes with a computer system that is exclusively for the use of critical infrastructure operations, or in the case in which such is not exclusively for the use of critical infrastructure operations, but it is used in critical infrastructure operations and such conduct affects that use or impacts the operations of critical infrastructure the punishment shall be imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.		Article 199 bis does not refer to the intent to alter or destroy being *"without right"* Further, Article 199 bis does not refer to the acts of intentional hindrance or distortion by *"inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data"* Referencing these acts will ensure that the offence describes what intentional hindrance or distortion means. **Gap Analysis** **Recommendation:** Use the BC language in Article 5 or section 9 HIPCAR - by adding *"intentional alters or destroys* ***without right****" and the acts of inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data"* Also consider whether the prevention and prosecution of attacks against critical infrastructure needs a separate or aggravated offence for example the functioning of a computer system may be hindered for terrorist purposes (e.g. hindering the system that stores stock exchange records can make them inaccurate, or hindering the functioning of critical infrastructure)[390] – section 9(2) HIPCAR for suggested wording

[390] http://www.coe.int/en/web/cybercrime/guidance-notes

Offences		
Budapest Convention on Cybercrime ('BC')	**National Legislation**	**Comments**
Article 6 BC[391] **Misuse of Devices** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a. the production, sale, procurement for use, import, distribution or otherwise making available of: i. i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5; ii. ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and b. the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.	**No equivalent**	**Legal Analysis** This offence will enable prosecution for the production, sale, procurement for use, import, distribution of access codes and other computerized data used to commit cybercrimes. - for example, computer systems may be accessed to facilitate a terrorist attack by interfering with a country's electrical power grid. This offence will enable prosecution for the production, sale, procurement for use, import, distribution of access codes and other computerized data used to commit cybercrimes. These are elements often present in malware prosecutions. Article 9 CITO makes no reference to *"without right"* – therefore – the wording of BC and HIPCAR is preferred. Any offence would also have to consider those devices that have a legitimate as well as being put to criminal use *("dual use")* – this should include the BC language of *"primarily adapted"* **Gap Analysis** **Recommendation:** Use the BC language in Article 6 or section 10 HIPCAR as a guide for national legislation. Please note that HIPCAR provides the option of listing the devices in a schedule if deemed appropriate – this could be restrictive and require updating with technological progress. The national law should provide a reasonable excuse so law enforcement can use devices for special investigation techniques – see the language at Article 6.2. BC or section 10(2) HIPCAR as a guide.

[391] Article 9 CITO and Article 29(1)(h) AUC

Offences		
Budapest Convention on Cybercrime ('BC')	**National Legislation**	**Comments**
2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system. 3. Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article. **Section 10 HIPCAR – Illegal Devices** 1. A person commits an offence if the person: a. intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, produces, sells, procures for use, imports, exports, distributes or otherwise makes available: i. a device, including a computer program, that is designed or adapted for the purpose of committing an offence defined by other provisions of Part II of this law; or ii. a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed;		

Offences		
Budapest Convention on Cybercrime ('BC')	National Legislation	Comments
with the intent that it be used by any person for the purpose of committing an offence defined by other provisions of Part II of this law; or b. has an item mentioned in subparagraph (i) or (ii) in his or her possession with the intent that it be used by any person for the purpose of committing an offence defined by other provisions of part II of this law commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. 2. This provision shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph I is not for the purpose of committing an offence established in accordance with other provisions of Part II of this law, such as for the authorized testing or protection of a computer system. 3. A country may decide not to criminalize illegal devices or limit the criminalization to devices listed in a Schedule.		

Offences		
Budapest Convention on Cybercrime ('BC')	**National Legislation**	**Comments**
Article 7 BC **Computer related forgery** Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches. **Section 11 HIPCAR – Computer-related Forgery** 1. A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification inputs, alters, deletes, or suppresses computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.	**Penal Code** **Article 172** A public servant or assimilated or a notary who, in the exercise of his functions, commits a forgery liable to cause public or private damage is punished by imprisonment for life and a fine of one thousand dinars, in the following cases : • by making, in whole or in part, a false document or deed, either by altering or distorting an original document by any means, either by affixing a counterfeit seal or signature, or by falsely attesting the identity or status of persons. • by making a false document or misrepresenting the truth by any means whatsoever on a material or immaterial medium, a computer or electronic document, a microfilm and a microfiche, the object of which is the proof of a right or of a fact giving rise to legal effects.	**Legal Analysis** The national offence only relates to public servants or a notary. Incorporation of BC article 7 is advised to protect against this offending which could include phishing and spear phishing. Language relevant to computer fraud should be used - for example *"computer data"* (such as the data used in electronic passports) may be input, altered, deleted, or suppressed with the result that inauthentic data is considered or acted upon for legal purposes as if it were authentic.[392] The language in the national legislation is vague with no reference to any dishonest intent and requires some form of "*damage*" without defining what this harm is – this is also the case with Article 10 CITO and the language in Article 7 BC and section 11 HIPCAR is to be preferred. Section 11(2) HIPCAR also provides for the sending of multiple electronic email messages as an aggravated offence. The language in Article 10 CITO has no reference to any dishonest intent and requires harm to be caused – the language in BC and HIPCAR is to be preferred as it does not require harm to be caused. BC and HIPCAR only requires that the "*inauthentic data*" data is "*considered*" **Gap Analysis** **Recommendation:** Use the BC language in Article 7 or section 11 HIPCAR as a guide for the national legislation A review as to whether *damage* needs to be an element of the offence – it is preferable not to use *damage* so that the forgery is committed as soon as the inauthentic data is created and *considered*. This would mean if a forged link or document is sent as part of a phishing scam the offence is complete as soon as the recipient *considers* it (i.e. opens the email containing the link or opens the attached document) – rather than having to prove the recipient has suffered any damage or harm

[392] http://www.coe.int/en/web/cybercrime/guidance-notes

Offences		
Budapest Convention on Cybercrime ('BC')	**National Legislation**	**Comments**
2. If the abovementioned offence is committed by sending out multiple electronic mail messages from or through computer systems, the penalty shall be imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. **Article 10 CITO** **Offence of Forgery** The use of information technology means to alter the truth of data in a manner that causes harm, with the intent of using them as true data. **Article 29(2)(b) AUC** Intentionally input, alter, delete, or suppress computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is directly readable and intelligible. A Party may require intent to defraud, of similar dishonest intent, before criminal liability attaches		
Article 8 BC[393] **Computer related fraud** Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by: a. any input, alteration, deletion or suppression of computer data, b. any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.		

[393] Article 11 CITO and Article 29(2)(d) AUC

Offences

Budapest Convention on Cybercrime ('BC')	National Legislation	Comments
Section 12 HIPCAR – Computer-related Fraud A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification causes a loss of property to another person by: - any input, alteration, deletion or suppression of computer data; - any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person the penalty shall be imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.	**Penal Code** **Article 199 ter** Anyone who has made a change of any kind whatsoever on the content of originally genuine computerized or electronic documents, provided that it is harmful to others….	**Legal Analysis** There is no definition of *"computerized", "electronic documents"* or *"harm"* in the national legislation and may create uncertainty. Article 199 ter has no reference to fraudulent dishonest intent without right - a computer fraud relates to a perpetrator intending to gain an economic benefit for himself or another. The fraudulent conduct without authorization in CITO is missing and may create uncertainty. There is no definition of *"harm"* or *"beneficiaries"* or *"illicitly"* in CITO, which may create greater uncertainty and fail to criminalize the conduct intended. Article 8 BC or section 12 HIPCAR is the preferred language **Gap Analysis** **Recommendation:** Providing definitions for *"computerized", "electronic documents" or "harm"* and ensure there is a fraudulent or dishonest intent without right – using language from BC or HIPCAR
Article 9 BC[394] **Content related offences (e.g. child pornography)** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a. producing child pornography for the purpose of its distribution through a computer system; b. offering or making available child pornography through a computer system; c. distributing or transmitting child pornography through a computer system; d. procuring child pornography through a computer system for oneself or for another person;	**Penal Code** **Article 226 bis** Anyone who publicly infringes morality or public morals by gesture or speech or intentionally interferes in a manner that infringes modesty is punished with six months' imprisonment and a fine of one thousand dinars. Anyone who publicly draws attention to an opportunity to commit the debauchery by writing, recording, audio or visual, electronic or optical messages is liable to the same penalties prescribed in the preceding paragraph.	**Legal Analysis** Article 9 BC and section 13 HIPCAR protect children from harm by criminalizing the distribution, transmitting, making available, offering, producing and possession of indecent images of children. Article 226bis does not refer to indecent images of children Organic Law No. 2016-61, dated on 3 August 2016, pertaining to the prevention and countering of human trafficking (trafficking in persons) does not specifically refer to child pornography – but rather prostitution of children and exploitation through pornographic scenes. This means the offence would relate to those who are involved in the prostitution of trafficked children to facilitate indecent images.

[394] Article 12 CITO and Article 29(3)(a-d) AUC

Offences		
Budapest Convention on Cybercrime ('BC')	**National Legislation**	**Comments**
e. possessing child pornography in a computer system or on a computer-data storage medium. 2. For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts: a. a minor engaged in sexually explicit conduct; b. a person appearing to be a minor engaged in sexually explicit conduct; c. realistic images representing a minor engaged in sexually explicit conduct. 3. For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years. 4. Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c. **Section 13 HIPCAR – Child Pornography** 1. A person who, intentionally, without lawful excuse or justification: • produces child pornography for the purpose of its distribution through a computer system; • offers or makes available child pornography through a computer system; • distributes or transmits child pornography through a computer system; • procures and/or obtain child pornography through a computer system for oneself or for another person;	**Organic Law No. 2016-61, dated on 3 August 2016, pertaining to the prevention and countering of human trafficking (trafficking in persons).** **Article 1** The purpose of this Act is to prevent all forms of exploitation by persons, including women and children, from combating trafficking, punishing the perpetrators and protecting and assisting victims. It also aims to promote national coordination and international cooperation in the fight against trafficking in persons within the framework of international, regional and bilateral conventions ratified by the Republic of Tunisia. Art. 2 - For the purposes of this Law, the following terms are used: 5 .... Economic or sexual exploitation of children in the course of their employment. 6 .... 7. Sexual exploitation: The obtaining of advantages of any kind whatever by giving a person to prostitution or any other type of sexual services in particular, its exploitation in pornographic scenes, through the production or possession or distribution, by any means, Scenes or pornographic material.	There is no definition of *"The obtaining of advantages of any kind"* **Gap Analysis** **Recommendation:** Article 9 BC or section 13 HIPCAR should be used as a precedent for national legislation

Offences		
Budapest Convention on Cybercrime ('BC')	**National Legislation**	**Comments**
- Possesses child pornography in a computer system or on a computer- data storage medium; or - knowingly obtains access, through information and communication technologies, to child pornography, commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. 2. It is a defense to a charge of an offence under paragraph (1) (b) to (1)(f) if the person establishes that the child pornography was a bona fide law enforcement purpose. 3. A country may not criminalize the conduct described in section 13 (1) (d)- (f).		
Article 10 BC [395] **Infringement of copyright** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.	**The law n° 2009-33 dated 23 June 2009, amending and completing law n° 94-36 dated 24 February 1994, relating to the literary and artistic property** [396]	**Legal Analysis** Law enforcement internationally utilizes digital copyright offences as additional criminal conduct to investigate and prosecute several forms of cybercrime (which include crimes such as phishing, electronic fraud, electronic forgery, fraudulent websites and data theft/data breaches). One of the underlying offences in many of these cases tends to be infringement of digital copyright. The Sony cyber attack[397] is only one recent example where offences and powers related to cybercrime, data theft/corporate espionage and copyright infringement came together to complement one another.

[395] Article 17 CITO and no equivalent in AUC

[396] Full text in English : http://www.legislation.tn/sites/default/files/fraction-journal-officiel/2009/2009G/052/Tg2009331.pdf or http://www.jurisitetunisie.com/tunisie/codes/prop_int/prop_int1000.html

[397] https://en.wikipedia.org/wiki/Sony_Pictures_hack

Offences		
Budapest Convention on Cybercrime ('BC')	**National Legislation**	**Comments**
2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system. 3. A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article. **Article 17 CITO - Offenses Related to Copyright and Adjacent Rights** Violation of copyright as defined according to the law of the State Party, if the act is committed deliberately and for no personal use, and violation of rights adjacent to the relevant copyright as defined according to the law of the State Party, if the act is committed deliberately and for no personal use.		Law n° 2009-33 dated 23 June 2009, amending and completing law n° 94-36 dated 24 February 1994 will protect innovation in the 21st century, businesses and citizens of Tunisia

Offences		
Budapest Convention on Cybercrime ('BC')	National Legislation	Comments
Article 11 BC[398] **Aiding and Abetting** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed. 2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention. **Article 19 CITO - Attempt at and Participation in the Commission of Offences** 1. Participation in the commission of any of the offences set forth in this chapter with the intention to commit the offence in the law of the State Party. 2. Attempt at the commission the offences set forth in Chapter II of this convention. 3. A State Party may reserve the right to not implement the second paragraph of this Article totally or partly.	**No equivalent**	**Legal Analysis** Aiding and abetting others to commit offences is essential in order to prosecute those who may have provided assistance or encouraged cybercrimes to take place. Article 19 CITO also includes attempt **Gap Analysis** **Recommendation:** Use Article 11 BC and Article 19 CITO (where no reference to attempt) as a guide for national legislation

[398] Article 29(2)(f) AUC

Offences		
Budapest Convention on Cybercrime ('BC')	**National Legislation**	**Comments**
Article 12 BC[399] **Corporate liability** 1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on: a. a power of representation of the legal person; b. an authority to take decisions on behalf of the legal person; c. an authority to exercise control within the legal person. 2. In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority. 3. Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative. 4. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.	**No equivalent**	**Legal Analysis** This provision is an essential element so that legal persons (e.g. corporate entities) acting on behalf of natural persons have criminal liability **Gap Analysis** **Recommendation:** Use the BC language in Article 12 as a guide for national legislation

[399] Article 20 CITO and Article 30(2) AUC

Offences		
Budapest Convention on Cybercrime ('BC')	National Legislation	Comments
Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems **Article 3[400] – Dissemination of racist and xenophobic material through computer systems** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: distributing, or otherwise making available, racist and xenophobic material to the public through a computer system. 2. A Party may reserve the right not to attach criminal liability to conduct as defined by paragraph 1 of this article, where the material, as defined in Article 2, paragraph 1, advocates, promotes or incites discrimination that is not associated with hatred or violence, provided that other effective remedies are available. 3. Notwithstanding paragraph 2 of this article, a Party may reserve the right not to apply paragraph 1 to those cases of discrimination for which, due to established principles in its national legal system concerning freedom of expression, it cannot provide for effective remedies as referred to in the said paragraph 2.	**Organic Law No. 2015-26 of 7 August 2015 on the fight against terrorism and the repression of money laundering.** **Article 14** Every person who commits, is guilty of a terrorist offense, First :......... Seventh: to cause damage to public or private property, vital resources, infrastructure, means of transport or communication, computer systems or public services, Eighth: accusation of apostasy or appeal, or incite, or incite hatred, animosity between races, doctrines and religions.	**Legal analysis** Article 14 of the national legislation does not specifically refer to dissemination through a computer system. The AUC Article 3(1)(e) - which includes the creation of and downloading racist and xenophobic material through a computer system rather than merely disseminating or making such material available - but does not include an intent or *"without right"* – the BC language is to be preferred. **Gap Analysis** **Recommendation:** Use the BC language in Article 3 Additional Protocol as a suggested precedent for national legislation

[400] Article 29(3)(e) AUC no equivalent in CITO

Offences		
Budapest Convention on Cybercrime ('BC')	**National Legislation**	**Comments**
Additional Protocol **Article 4[401] – Racist and xenophobic motivated threat** Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: threatening, through a computer system, with the commission of a serious criminal offence as defined under its domestic law, (i) persons for the reason that they belong to a group, distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors, or (ii) a group of persons which is distinguished by any of these characteristics.	**No equivalent**	**Gap Analysis** **Recommendation:** Use the BC language in Article 4 Additional Protocol as a guide for national legislation
Additional Protocol **Article 5[402] - Racist and xenophobic motivated insult** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: insulting publicly, through a computer system, (i) persons for the reason that they belong to a group distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors; or (ii) a group of persons which is distinguished by any of these characteristics.	**No equivalent**	**Gap Analysis** **Recommendation:** Use the BC language in Article 5 Additional Protocol as a guide for national legislation

[401] Article 29(3)(f) AUC no equivalent in CITO

[402] Article 29(3)(g) AUC no equivalent in CITO

Offences		
Budapest Convention on Cybercrime ('BC')	**National Legislation**	**Comments**
2. A Party may either: a. require that the offence referred to in paragraph 1 of this article has the effect that the person or group of persons referred to in paragraph 1 is exposed to hatred, contempt or ridicule; or b. reserve the right not to apply, in whole or in part, paragraph 1 of this article.		
Additional Protocol **Article 6[403] - Denial, gross minimisation, approval or justification of genocide or crimes against humanity** 1. Each Party shall adopt such legislative measures as may be necessary to establish the following conduct as criminal offences under its domestic law, when committed intentionally and without right: distributing or otherwise making available, through a computer system to the public, material which denies, grossly minimises, approves or justifies acts constituting genocide or crimes against humanity, as defined by international law and recognised as such by final and binding decisions of the International Military Tribunal, established by the London Agreement of 8 August 1945, or of any other international court established by relevant international instruments and whose jurisdiction is recognised by that Party.	**No equivalent**	**Gap Analysis** **Recommendation:** Use the BC language in Article 6 Additional Protocol as a guide for national legislation

[403] Article 29(3)(h) AUC no equivalent in CITO

<table>
<tr><th colspan="3">Offences</th></tr>
<tr><th>Budapest Convention on Cybercrime ('BC')</th><th>National Legislation</th><th>Comments</th></tr>
<tr><td>2. A Party may either
a. require that the denial or the gross minimisation referred to in paragraph 1 of this article is committed with the intent to incite hatred, discrimination or violence against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors, or otherwise
b. reserve the right not to apply, in whole or in part, paragraph 1 of this article.</td><td></td><td></td></tr>
<tr><th colspan="3">Additional Offences to Review</th></tr>
<tr><td><b>Identity-related Crimes</b>
<b>Section 14 HIPCAR</b>
A person who, intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification by using a computer system in any stage of the offence, intentionally transfers, possesses, or uses, without lawful excuse or justification, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a crime, commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.</td><td></td><td><b>Legal Analysis</b>
This offence covers the preparation phase of an identity –related crime of dishonesty
<b>Gap Analysis</b>
<b>Recommendation:</b> Inclusion in domestic legislation is advisable.</td></tr>
</table>

Offences		
Budapest Convention on Cybercrime ('BC')	**National Legislation**	**Comments**
Disclosure of Details of an Investigation **Section 16 HIPCAR** An Internet service provider who receives an order related to a criminal investigation that explicitly stipulates that confidentiality is to be maintained or such obligation is stated by law and intentionally without lawful excuse or justification or in excess of a lawful excuse or justification discloses: • the fact that an order has been made; or • anything done under the order; or • any data collected or recorded under the order; commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.		**Legal Analysis** This offence sanctions data breaches and disclosure of sensitive information that could impact criminal investigations **Gap Analysis** **Recommendation:** Inclusion in domestic legislation is advisable.
Failing to Permit Assistance **Section 17 HIPCAR** 1. A person other than the suspect who intentionally fails without lawful excuse or justification or in excess of a lawful excuse or justification to permit or assist a person based on an order as specified by sections 20 to 22[404] commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both. 2. A country may decide not to criminalize the failure to permit assistance provided that other effective remedies are available.		**Legal Analysis** This offence relates to persons, with specific knowledge of relevant evidence, who refuse to assist. Often law enforcement will be reliant upon such persons to secure evidence in cyber investigations. A separate offence is the failure to provide passwords or access to codes to encrypted devices or data (i.e. *"key to protected information")* – section 53 of the UK Regulation of Investigatory Powers Act 2000 (RIPA) [405] provides for a criminal offence for persons who fail to comply with a section 49 RIPA Notice to disclose the *"key"* **Gap Analysis** **Recommendation:** Inclusion in domestic legislation is advisable.

[404] Search and seizure, assistance and production orders

[405] http://www.legislation.gov.uk/ukpga/2000/23/section/53

Offences		
Budapest Convention on Cybercrime ('BC')	National Legislation	Comments
Cyber Stalking **Section 18 HIPCAR** A person, who without lawful excuse or justification or in excess of a lawful excuse or justification initiates any electronic communication, with the intent to coerce, intimidate, harass, or cause substantial emotional distress to a person, using a computer system to support severe, repeated, and hostile behavior, commits an offence punishable, on conviction, by imprisonment for a period not exceeding [period], or a fine not exceeding [amount], or both.		**Legal Analysis** This offence criminalizes those who harass persons online– some jurisdictions may have non-computer related harassment offences – but this offence is recommended for those crimes committed online. **Gap Analysis** **Recommendation:** Inclusion in domestic legislation is advisable.
Grooming Children Online **Dutch Criminal Code 248e** The person who proposes to arrange a meeting, by means of an automated work or by making use of a communication service, to a person of whom he knows, or should reasonably assume, that such person has not yet reached the age of sixteen, with the intention of committing indecent acts with this person or of creating an image of a sexual act in which this person is involved, will be punished with a term of imprisonment of at most two years or a fine of the fourth category, if he undertakes any action intended to realise that meeting. **Canadian Criminal Code** **Section 172.1** 1. Every person commits an offence who, by a means of telecommunication, communicates with		**Legal Analysis** To prove the Dutch offence a meeting for sexual purposes is required with supporting evidence of online chat history with sexual intent; request for a meeting with evidence this was planned (i.e. date and place). The purpose of the Canadian law is to prevent grooming by predatory adults of children online. This offence does not require the sexual offence to have occurred. This means the accused does not need to have actually gone to meet the victim in person. The offence is committed before any actions are taken to commit the substantive offence. **Gap Analysis** **Recommendation:** Inclusion in domestic legislation is advisable to criminalise this preparatory behaviour before a sexual offence is committed

Offences		
Budapest Convention on Cybercrime ('BC')	National Legislation	Comments
a. a person who is, or who the accused believes is, under the age of 18 years, for the purpose of facilitating the commission of an offence under subsection 153(1), section 155, 163.1, 170 or 171 or subsection 212(1), (2), (2.1) or (4) with respect to that person; b. a person who is, or who the accused believes is, under the age of 16 years, for the purpose of facilitating the commission of an offence under section 151 or 152, subsection 160(3) or 173(2) or section 271, 272, 273 or 280 with respect to that person; or c. a person who is, or who the accused believes is, under the age of 14 years, for the purpose of facilitating the commission of an offence under section 281 with respect to that person. Punishment 2. Every person who commits an offence under subsection (1) is guilty of a. is guilty of an indictable offence and is liable to imprisonment for a term of not more than 10 years and to a minimum punishment of imprisonment for a term of one year; or b. is guilty of an offence punishable on summary conviction and is liable to imprisonment for a term of not more than 18 months and to a minimum punishment of imprisonment for a term of 90 days.		

Offences		
Budapest Convention on Cybercrime ('BC')	**National Legislation**	**Comments**
Presumption re age 3. Evidence that the person referred to in paragraph (1)(a), (b) or (c) was represented to the accused as being under the age of eighteen years, sixteen years or fourteen years, as the case may be, is, in the absence of evidence to the contrary, proof that the accused believed that the person was under that age. No defence 4. It is not a defence to a charge under paragraph (1)(a), (b) or (c) that the accused believed that the person referred to in that paragraph was at least eighteen years of age, sixteen years or fourteen years of age, as the case may be, unless the accused took reasonable steps to ascertain the age of the person.		

Procedure		
International Best Practice	**National Legislation**	**Comments**
Article 19 BC[406] **Search and seizure of stored computer data** 1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access: a. a computer system or part of it and computer data stored therein; and b. a computer-data storage medium in which computer data may be stored in its territory.	**No equivalent**	**Legal Analysis** This is the most essential investigatory power and should refer to gaining access than search. In the BC Explanatory Report, *"Search"* means to seek, read, inspect or review data. It includes the notion of searching for data and searching of (examining) data. The word *"access"* has a neutral meaning and reflects more accurately computer terminology – this is also included in Articles 26 and 27 CITO.[407]

[406] Article 3 AUC

[407] Paragraph 191, page 33 Explanatory Report BC

Procedure		
International Best Practice	**National Legislation**	**Comments**
2. Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system. 3. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to: a. seize or similarly secure a computer system or part of it or a computer-data storage medium; b. make and retain a copy of those computer data; c. c maintain the integrity of the relevant stored computer data; d. d render inaccessible or remove those computer data in the accessed computer system.		**Gap Analysis** **Recommendation:** The national legislation could incorporate relevant language from BC and HIPCAR to include definitions of a *computer system*[408] and *computer data*[409] and refer consistently to *access* There should be a definition of "*seize*" to insure integrity and to specific procedures - section 3(16) HIPCAR "*Seize includes:* • *activating any onsite computer system and computer data storage media;* • *making and retaining a copy of computer data, including by using onsite equipment;* • *maintaining the integrity of the relevant stored computer data;* • *rendering inaccessible, or removing, computer data in the accessed computer system;* • *taking a printout of output of computer data; or* • *seize or similarly secure a computer system or part of it or a computer- data storage medium.*" Section 21 HIPCAR provides for legislation to ensure assistance is provided by those who have specialist knowledge of the location of relevant evidence – this could be used as a guide – also see section 17 HIPCAR for an offence if assistance is refused without lawful excuse

[408] See Article 1.a. BC: "*any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data*" **or** section 3(5) HIPCAR: "*a device or a group of inter-connected or related devices, including the Internet, one or more of which, pursuant to a program, performs automatic processing of data or any other function.*"

[409] See Article 1.b. BC: "*any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function*" **or** section 3(6) HIPCAR: "*Computer data means any representation of facts, concepts, information (being either texts, sounds or images) machine-readable code or instructions, in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.*"

Procedure		
International Best Practice	National Legislation	Comments
4. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2. 5. The powers and procedures referred to in this article shall be subject to Articles 14 and 15. **Section 20 HIPCAR – Search and Seizure** 1. If a [judge] [magistrate] is satisfied on the basis of [information on oath] [affidavit] that there are reasonable grounds [to suspect] [to believe] that there may be in a place a thing or computer data: • that may be material as evidence in proving an offence; or • that has been acquired by a person as a result of an offence; the [judge] [magistrate] [may] [shall] issue a warrant authorizing a [law enforcement] [police] officer, with such assistance as may be necessary, to enter the place to search and seize the thing or computer data including search or similarly access: i. a computer system or part of it and computer data stored therein; and		

Procedure		
International Best Practice	**National Legislation**	**Comments**
ii. a computer-data storage medium in which computer data may be stored in the territory of the country. 2. If [law enforcement] [police] officer that is undertaking a search based on Sec. 20 (1) has grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, he shall be able to expeditiously extend the search or similar accessing to the other system. 3. A [law enforcement] [police] officer that is undertaking a search are empowered to seize or similarly secure computer data accessed according to paragraphs 1 or 2. **Section 21 HIPCAR – Assistance** Any person who is not a suspect of a crime but who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein that is the subject of a search under section 20 must permit, and assist if reasonably required and requested by the person authorized to make the search by: • providing information that enables the undertaking of measures referred to in section 20; • accessing and using a computer system or computer data storage medium to search any computer data available to or in the system; • obtaining and copying such computer data; • using equipment to make copies; and		

Procedure		
International Best Practice	**National Legislation**	**Comments**
• obtaining an intelligible output from a computer system in such a format that is admissible for the purpose of legal proceedings. **Article 26 CITO - Inspecting Stored Information** 1. Every State Party shall commit itself to adopting the procedures necessary to enable its competent authorities to inspect or access: a. an information technology or part thereof and the information stored therein or thereon. b. the storage environment or medium in or on which the information may be stored. 2. Every State Party shall commit itself to adopting the procedures necessary to enable the competent authorities to inspect or access a specific information technology or part thereof in conformity with paragraph 1(a) if it is believed that the required information is stored in another information technology or in part thereof in its territory and such information is legally accessible or available in the first technology, the scope of inspection may be extended and the other technology accessed. **Article 27 CITO - Seizure of Stored Information** 1. Every State Party shall commit itself to adopting the procedures necessary to enable the competent authorities to seize and safeguard information technology information accessed according to Article 26, paragraph 1, of this Convention. These procedures include the authority to:		

Procedure		
International Best Practice	National Legislation	Comments
a. seize and safeguard the information technology or part thereof or the storage medium for the information technology information. b. make a copy the information technology information and keep it. c. maintain the integrity of the stored information technology information. d. remove such accessed information from the information technology or prevent its access. 2. Every State Party shall commit itself to adopting the procedures necessary to enable the competent authorities to order any person who is acquainted with the functioning of the information technology or the procedures applied to protect the information technology to give the information necessary to complete the procedures mentioned in paragraphs 2 and 3 of Article 26 of this Convention.		
Article 16 BC[410] **Expedited preservation of stored computer data** 1. Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.	**No equivalent**	**Legal Analysis** This procedural power is important to ensure that data which is vulnerable to deletion or loss is preserved

[410] no equivalent in AUC

Procedure		
International Best Practice	**National Legislation**	**Comments**
2. Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed. 3. Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law. 4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15.		**Gap Analysis** **Recommendation:** This expedited power to retain BSI, metadata, transactional and stored content is essential as part of cybercrime investigations to ensure the evidence is available for search, access, seizure and review. The language of Article 16 of the BC, section 23 HIPCAR or Article 23 CITO could be used. The national legislation will require sufficient definitions of *"subscriber information or BSI",*[411] *"traffic data"*[412] *and "Communication Service Provider"*[413] to ensure it can be preserved. Consideration should be given the length of preservation that is reasonable in the circumstances and allowing for an application to extend in exigent circumstances – BC and CITO have 90 days and HIPCAR 7 days. From experience 90 days is too few in a cyber investigation and the figure should be nearer 180 days and then subject to extension.

[411] See Article 2(9) CITO: *"Any information that the service provider has concerning the subscribers to the service, except for information through which the following can be known: a. the type of communication service used, the technical requirements and the period of service. b. the identity of the subscriber, his postal or geographic address or phone number and the payment information available by virtue of the service agreement or arrangement. c. any other information on the installation site of the communication equipment by virtue of the service agreement."*

[412] See Article 1.d BC: *"any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service"* **or** section 3(18) HIPCAR: *"Traffic data means computer data that: a. relates to a communication by means of a computer system; and b. is generated by a computer system that is part of the chain of communication ; and c. shows the communication's origin, destination, route, time date, size, duration or the type of underlying services."*

[413] See Article 1.c.BC: *"i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and ii any other entity that processes or stores computer data on behalf of such communication service or users of such service"* **or** Article 2(2) CITO: *"any natural or juridical person, common or private, who provides subscribers with the services needed to communicate through information technology, or who processes or stores information on behalf of the communication service or its users."*

Procedure		
International Best Practice	National Legislation	Comments
Section 23 HIPCAR – Expedited Preservation If a [law enforcement] [police] officer is satisfied that there are grounds to believe that computer data that is reasonably required for the purposes of a criminal investigation is particularly vulnerable to loss or modification, the [law enforcement] [police] officer may, by written notice given to a person in control of the computer data, require the person to ensure that the data specified in the notice be preserved for a period of up to seven (7) days as specified in the notice. The period may be extended beyond seven (7) days if, on an ex parte application, a [judge] [magistrate] authorizes an extension for a further specified period of time. **Article 23 CITO - Expeditious Custody of Data Stored in Information Technology** 1. Every State Party shall adopt the procedures necessary to enable the competent authorities to issue orders or obtain the expeditious custody of information, including information for tracking users, that was stored on an information technology, especially if it is believed that such information could be lost or amended.		

Procedure		
International Best Practice	**National Legislation**	**Comments**
2. Every State Party shall commit itself to adopting the procedures necessary as regards paragraph 1, by means of issuing an order to a person to preserve the information technology information in his possession or under his control, in order to require him to preserve and maintain the integrity of such information for a maximum period of 90 days that may be renewed, in order to allow the competent authorities to search and investigate 3. Every State Party shall commit itself to adopting the procedures necessary to require the person responsible for safeguarding the information technology to maintain the procedures secrecy throughout the legal period stated in the domestic law.		
Article 17 BC[414] **Expedited preservation and partial disclosure of traffic data** 1. Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to: a. ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and	**No equivalent**	**Legal Analysis** This procedural power is especially important to ensure that CSPs provide IP addresses that could locate the perpetrator of a cybercrime. **Gap Analysis** **Recommendation:** This expedited power alongside disclosure of traffic data should be included in legislation to enable effective investigations of cybercrime. The language of Article 17 of the BC, sections 23 and 24 HIPCAR or Article 24 CITO could be used. This will also require definitions of *"traffic data" and "Communication Service Provider"*[415]

[414] no equivalent in AUC

[415] See definitions above

Procedure		
International Best Practice	**National Legislation**	**Comments**
b. ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted. 2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15. **Section 23 HIPCAR – Expedited Preservation** If a [law enforcement] [police] officer is satisfied that there are grounds to believe that computer data that is reasonably required for the purposes of a criminal investigation is particularly vulnerable to loss or modification, the [law enforcement] [police] officer may, by written notice given to a person in control of the computer data, require the person to ensure that the data specified in the notice be preserved for a period of up to seven (7) days as specified in the notice. The period may be extended beyond seven (7) days if, on an ex parte application, a [judge] [magistrate] authorizes an extension for a further specified period of time.		

Procedure		
International Best Practice	National Legislation	Comments
Section 24 HIPCAR – Partial Disclosure of Traffic Data If a [law enforcement] [police] officer is satisfied that data stored in a computer system is reasonably required for the purposes of a criminal investigation, the [law enforcement] [police] officer may, by written notice given to a person in control of the computer system, require the person to disclose sufficient traffic data about a specified communication to identify: a. the Internet service providers; and/or b. the path through which the communication was transmitted. **Article 24 CITO - Expeditious Custody and Partial Disclosure of Users Tracking Information** Every State Party shall commit itself to adopting the procedures necessary as regards users tracking information in order to: 1. ensure expeditious custody of users tracking information, regardless of whether such communication is transmitted by one or more service providers. 2. ensure that a sufficient amount of users tracking information is disclosed to the competent authorities of the State Party or to a person appointed by these authorities to allow the State Party to determine the service providers and the transmission path of the communications.		

Procedure		
International Best Practice	**National Legislation**	**Comments**
Article 18 BC[416] **Production Order** 1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order: a. a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and b. a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control. 2. The powers and procedures referred to in this article shall be subject to Articles 14 and 15. 3. For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a. the type of communication service used, the technical provisions taken thereto and the period of service;		**Legal Analysis** This is an essential provision for an effective cybercrime investigation and its absence will impact upon prosecutions and international cooperation. **Gap Analysis** **Recommendation:** This essential power is necessary to ensure CSPs in Tunisia provide BSI, traffic data and stored content data. This will also require definitions of *"computer data", "subscriber information or BSI", "traffic data"* and *"Communication Service Provider"*.[417] Article 25 CITO is a model that could be used and uses different definitions including *"information technology"*,[418] *"service provider"*[419] and *"data"*[420] – it is still advisable to have definitions for *"subscriber information or BSI", "traffic data"* as they will be different types of evidence that can be produced from CSPs. Further, this power will require individuals and others (such as corporate entities, financial institutions and other organisations) who hold data to produce it to law enforcement authorities. Article 18 BC and section 22 HIPCAR could be a guide with consistent application of definitions

[416] no equivalent in AUC

[417] See definitions above

[418] Article 2(1) CITO: "*any material or virtual means or group of interconnected means used to store, sort, arrange, retrieve, process, develop and exchange information according to commands and instructions stored therein. This includes all associated inputs and outputs, by means of wires or wirelessly, in a system or network.*"

[419] Article 2(2) CITO see above

[420] Article 2(3) CITO: "*all that may be stored, processed, generated and transferred by means of information technology, such as numbers, letters, symbols, etc…*"

Procedure		
International Best Practice	National Legislation	Comments
b. the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement; c. any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement. **Section 22 HIPCAR – Production Order** If a [judge] [magistrate] is satisfied on the basis of an application by a [law enforcement] [police] officer that specified computer data, or a printout or other information, is reasonably required for the purpose of a criminal investigation or criminal proceedings, the [judge] [magistrate] may order that: • a person in the territory of [enacting country] in control of a computer system produce from the system specified computer data or a printout or other intelligible output of that data; or • an Internet service provider in [enacting country] to produce information about persons who subscribe to or otherwise use the service. **Article 25 CITO - Order to Submit Information** Every State Party shall commit itself to adopting the procedures necessary to enable the competent authorities to issue orders to:		

Procedure		
International Best Practice	**National Legislation**	**Comments**
1. Any person in its territory to submit certain information in his possession which is stored on information technology or a medium for storing information. 2. Any service provider offering his services in the territory of the State Party to submit user's information related to that service which is in the possession of the service provider or under his control.	**No equivalent**	
Article 21 BC[421] **Interception of content data** 1. Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to: a. collect or record through the application of technical means on the territory of that Party, and b. compel a service provider, within its existing technical capability: i. to collect or record through the application of technical means on the territory of that Party, or ii. to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system.	**Organic Law No. 2016-61, dated on 3 August 2016, pertaining to the prevention and countering of human trafficking (trafficking in persons).** **Article 42** Any person, except those authorized by law, who intentionally intercepts communications and correspondence or audiovisual surveillance disregarding legal provisions, shall punished by five years' imprisonment and a fine of five thousand dinars. The attempt shall be punishable. **Organic Law No. 2015-26 of 7 August 2015 on the fight against terrorism and the repression of money laundering.** **Article 64** Any person, except those authorized by law, who intentionally intercepts communications and correspondence or audiovisual surveillance disregarding legal provisions, shall punished by five years' imprisonment and a fine of five thousand dinars. The attempt shall be punishable.	**Legal Analysis** This power is essential for national legislation – and there must be safeguards and requirement/procedure to compel CSPs cooperation to collect or record content data in real-time of specific communications in Tunisia. The national legislation does not contain explicit provisions concerning a real-time collection of data. Although the restriction on the use of interception technique criminalized in Article 42 of Organic Law No. 2016-61 and Article 64 of Organic Law No. 2015-26 **Gap Analysis** **Recommendations:** Provision should be made to compel CSPs in Tunisia to cooperate with real-time collection of content; and safeguards should be incorporated to ensure the collection is legal, necessary, reasonable and proportionate in the circumstances. Consideration should be given to reviewing Article 29 of CITO, Article 21 BC and section 26 HIPCAR and incorporating language in national legislation

[421] no equivalent in AUC

Procedure		
International Best Practice	**National Legislation**	**Comments**
2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory. 3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15. **Section 26 HIPCAR – Interception of Content Data** 1. If a [judge] [magistrate] is satisfied on the basis of [information on oath] [affidavit] that there are reasonable grounds to [suspect] [believe] that the content of electronic communications is reasonably required for the purposes of a criminal investigation, the magistrate [may] [shall]: • order an Internet service provider whose service is available in [enacting country] through application of technical means to collect or record or to permit or assist competent authorities with the collection or recording of content data associated with specified communications transmitted by means of a computer system; or		

Procedure		
International Best Practice	**National Legislation**	**Comments**
• authorize a [law enforcement] [police] officer to collect or record that data through application of technical means. 2. A country may decide not to implement section 26. **Article 29 CITO - Interception of Content Information** 1. Every State Party shall commit itself to adopting the legislative procedures necessary as regards a series of offences set forth in the domestic law, in order to enable the competent authorities to: a. gather or register through technical means in the territory of this State Party, or b. cooperate with and help the competent authorities to expeditiously gather and register content information of the relevant communications in its territory and which are transmitted by means of the information technology. 2. If, because of the domestic legal system, the State Party is unable to adopt the procedures set forth in paragraph 1(a), it may adopt other procedures in the form necessary to ensure the expeditious gathering and registration of content information corresponding to the relevant communications in its territory using the technical means in that territory. 3. Every State Party shall commit itself to adopting the procedures necessary to require the service provider to maintain the secrecy of any information when exercising the authority set forth in this Article.		

Procedure		
International Best Practice	**National Legislation**	**Comments**
Article 20 BC[422] **Real-time collection of traffic data** 1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to: a. collect or record through the application of technical means on the territory of that Party, and b. compel a service provider, within its existing technical capability: i. to collect or record through the application of technical means on the territory of that Party; or ii. to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system. 2. Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.	**No equivalent**	**Legal Analysis** There is no procedural power just to collect traffic data real-time. There could be a lower threshold to collect real-time traffic data which is an essential investigative tool. There may be situations where a higher legal threshold to secure content is not made out by an applicant – but a lower threshold to secure traffic could be. For this reason, there should be a distinction between real-time collection of stored content and traffic data. There must be safeguards and requirements/procedure to compel CSPs cooperation to collect or record content data in real-time of specific communications in Tunisia **Gap Analysis** **Recommendations:** There should be a specific power to collect traffic data real-time and provision should be made to compel CSPs in Tunisia to cooperate with real-time collection of traffic data; and safeguards should be incorporated to ensure the collection is legal, necessary, reasonable and proportionate in the circumstances. The language from Article 28 CITO could be considered but this does not refer to real-time only expeditious collection. Article 20 BC and section 25 HIPCAR should be used as a guide for national legislation

[422] Article 31(3)(e) – Note Article 28 CITO refers to expeditious collection rather than real-time collection

Procedure		
International Best Practice	**National Legislation**	**Comments**
3. Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it. 4. The powers and procedures referred to in this article shall be subject to Articles 14 and 15. **Section 25 HIPCAR - Collection of Traffic Data** 1. If a [judge] [magistrate] is satisfied on the basis of [information on oath][affidavit] that there are reasonable grounds to [suspect] [believe] that traffic data associated with a specified communication is reasonably required for the purposes of a criminal investigation, the [judge] [magistrate] [may] [shall] order a person in control of such data to: a. collect or record traffic data associated with a specified communication during a specified period; or b. permit and assist a specified [law enforcement] [police] officer to collect or record that data. 2. If a [judge] [magistrate] is satisfied on the basis of [information on oath] [affidavit] that there are reasonable grounds to [suspect] [believe] that traffic data is reasonably required for the purposes of a criminal investigation, the [judge] [magistrate] [may] [shall] authorize a [law enforcement] [police] officer to collect or record traffic data associated with a specified communication during a specified period through application of technical means. 3. A country may decide not to implement section 25.		

Procedure		
International Best Practice	**National Legislation**	**Comments**
		Disclosure obligation of encryption keys With terrorists and organized criminals routinely using encrypted messaging applications[423] this may be considered a viable power to release the keys to passwords to unlock devices[424] **Gap Analysis** **Recommendation:** Unable to clarify if there were any such powers in Tunisia– but such a power will allow law enforcement to compel owners to unlock devices
		Data retention obligations[425] Such a power can allow law enforcement to 1. Trace and identify the source of a communication 2. Identify the destination of a communication; 3. Identify the date, time and duration of a communication; and 4. Identify the type of communication Tunisia does have such an obligation[426]

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
Article 22 BC **Jurisdiction** 1. Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed: a. in its territory; or	**No equivalent**	**Legal Analysis** Without a clearly defined scope for cybercrime offences, that are international in nature, any legislation will be restricted. **Gap Analysis** **Recommendation:** National legislation ensures jurisdiction is defined using the language of Article 22 BC, section 19 HIPCAR or Article 30 CITO.

[423] Eleanor Saitta. "Can Encryption Save Us?" Nation 300, no. 24 (June 15, 2015): 16-18. Academic Search Premier, EBSCOhost (accessed February 29, 2016).

[424] For an example see section 49 Regulation of Investigatory Powers Act 2000 (UK) - http://www.legislation.gov.uk/ukpga/2000/23/section/49

[425] In 2006 the EU issued its Data Retention Directive - EU Member States had to store electronic telecommunications data for at least six months and at most 24 months for investigating, detecting and prosecuting serious crime. In 2014, the Court of Justice of the EU invalidated the Data Retention Directive, holding that it provided insufficient safeguards against interferences with the rights to privacy and data protection. In the absence of a valid EU Data Retention Directive, Member States may still provide for a data retention scheme – for national schemes see: http://fra.europa.eu/en/theme/information-society-privacy-and-data-protection/data-retention

[426] ICMEC Global Review page 40

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
b. on board a ship flying the flag of that Party; or c. on board an aircraft registered under the laws of that Party; or d. by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State. 2. Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof. 3. Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition. 4. This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law. 5. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.		If there is a conflict between jurisdictions consideration should be given to guidelines on determining the appropriate jurisdiction to try an offence – see the Eurojust Guidelines for Deciding which Jurisdiction should Prosecute (revised 2016)[427]

[427] http://www.eurojust.europa.eu/Practitioners/operational/Documents/Operational-Guidelines-for-Deciding.pdf

International Cooperation		
International Best Practice	National Legislation	Comments
Section 19 HIPCAR – Jurisdiction This Act applies to an act done or an omission made: • in the territory of [enacting country]; or • on a ship or aircraft registered in [enacting country]; or • by a national of [enacting country] outside the jurisdiction of any country; or by a national of [enacting country] outside the territory of [enacting country], if the person's conduct would also constitute an offence under a law of the country where the offence was committed. **Article 30 CITO - Competence** 1. 1.Every State Party shall commit itself to adopting the procedures necessary to extend its competence to any of the offences set forth in Chapter II of this Convention, if the offence is committed, partly or totally, or was realized: a. in the territory of the State Party b. on board a ship raising the flag of the State Party. c. on board a plane registered under the law of the State Party. d. by a national of the State Party if the offence is punishable according to the domestic law in the location where it was committed, or if it was committed outside the jurisdiction of any State. e. if the offence affects an overriding interest of the State.		

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
2. Every State Party shall commit itself to adopting the procedures necessary to extend the competence covering the offences set forth in Article 31, paragraph 1, of this Convention in the cases in which the alleged offender is present in the territory of that State Party and shall not extradite him to another Party according to his nationality following the extradition request. 3. If more than one State Party claim to have jurisdiction over an offence set forth in this Convention, priority shall be accorded to the request of the State whose security or interests were disrupted by the offence, followed by the State in whose territory the offence was committed, and then by the State of which the wanted person is a national. In case of similar circumstances, priority shall be accorded to the first State that requests the extradition.		
Article 35 BC[428] **24/7 Network** 1. Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:	**No equivalent**	**Legal Analysis** This is an essential mechanism for an effective cybercrime investigative capability. **Gap Analysis** **Recommendation:** This should not require legislation to implement and subject to resources should be established as a priority. Contact details should be shared for the nominated single point of contact (SPOC) nationally, central authorities internationally and INTERPOL. Consideration should also be given to drafting a Memorandum of Understanding with national agencies so that the SPOC has authority to undertake the actions required as part of an international cybercrime investigation applying national laws and treaties. This MOU will include both incoming and outgoing requests and ensure an efficient and effective process.

[428] Article 43 CITO

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
a. the provision of technical advice; b. the preservation of data pursuant to Articles 29 and 30; c. the collection of evidence, the provision of legal information, and locating of suspects. 2. a. A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis. b. If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to coordinate with such authority or authorities on an expedited basis. 3. Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.		
Article 25 BC **General principles relating to mutual assistance** 1. The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.		**Legal Analysis** *Article 25 BC ensures that it can be used as an instrument to facilitate MLA.*[429] Tunisia is not a party to the BC, CITO or AUC. This means that Tunisia is not a party to an international convention dedicated to cybercrime, and this will hinder international investigations as procedural powers will not have a legal basis. Other than any bilateral treaty – Tunisia is a signatory to UNTOC[430] so Article 18 UNTOC is the basis for MLA and mutuality/reciprocity.[431]

[429] there is no equivalent provision in the AUC

[430] Ratified 19 June 2003

[431] UNTOC Article 18 could be the basis for MLA if definition of transnational organized crime satisfied and also Riyadh Agreement on Judicial Cooperation could be a basis to States who have ratified

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
2. Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35. 3. Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication. 4. Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.		This means that without national legislation requests cannot be made for expedited preservation of stored computer data, expedited preservation and partial disclosure of traffic data and disclosure of stored data and traffic data, meaning a limitation to the international cooperation that Tunisia can provide to Requesting States. See Annex A for the types of international requests sent by Tunisia. **Gap Analysis** **Recommendation:** Domestic law is required for expedited preservation of stored computer data, expedited preservation and partial disclosure of traffic data and production orders**.** The BC, HIPCAR and CITO can be used as precedents for expedited preservation of stored computer data,[432] expedited preservation and partial disclosure of traffic data[433] disclosure of stored data[434] and expedited gathering of traffic data[435] - there also needs to be consideration of provision for real-time interception of traffic data and content[436]. Further, there needs to be a framework to cooperate on cybercrime investigations provided by multilateral conventions such as Article 27 BC and Article 32 CITO.[437] Consideration should be given to allowing adjudicating authorities to authorise domestic law enforcement to investigate in the State where access to a device is known. Accessibility of information is the essential criterion to initiate an investigation in cases where it is not possible to know where the data is stored (i.e. in the cloud). This could include a "mutual recognition" of court orders issued towards communication service providers in a given State, that could be served to branches of that CSPs located in other States, depending on where the data is stored.

[432] Article 29 BC, section 23 HIPCAR and Article 37 CITO

[433] Article 30 BC, sections 23 and 24 HIPCAR and Article 38 CITO

[434] Article 31 BC and Article 39 CITO

[435] Article 41 CITO

[436] Article 33 and 34 BC and sections 25 and 26 HIPCAR

[437] There are no equivalent provisions on the procedure for MLA in AUC

International Cooperation		
International Best Practice	National Legislation	Comments
5. Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws. **Article 34 CITO - Procedures for Cooperation and Mutual Assistance Requests** 1. The provisions of paragraphs 2-9 of this Article shall apply in case no cooperation and mutual assistance treaty or convention exists on the basis of the applicable legislation between the State Parties requesting assistance and those from which assistance is requested. If such a treaty or convention exists, the mentioned paragraphs shall not apply, unless the concerned parties agree to apply them in full or in part. 2. a. Every State Party shall designate a central authority responsible for sending and responding to mutual assistance requests and for their implementation and referral to the relevant authorities for implementation. b. Central authorities shall communicate directly among themselves.		

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
c. Every State Party shall, at the time of signature or deposit of the instrument of ratification, acceptance or agreement, contact the General Secretariat of the Council of Arab Interior Ministers and the Technical Secretariat of the Arab Justice Ministers and communicate to them the names and addresses of the authorities specifically designated for the purposes of this paragraph. d. The General Secretariat of the Council of Arab Interior Ministers and the Technical Secretariat of the Arab Justice Ministers shall establish and update a registry of concerned central authorities appointed by the State Parties. Every State Party shall insure that the registry's details are correct at all times 3. Mutual assistance requests in this Article shall be implemented according to procedures specified by the requesting State Party, except in the case of non conformity with the law of the State Party from which assistance is requested. 4. The State Party from which assistance is requested may postpone taking action on the request if such action shall affect criminal investigations conducted by its authorities. 5. Prior to refusing or postponing assistance, the State Party from which assistance is requested shall decide, after consulting with the requesting State Party, whether the request shall be partially fulfilled or be subject to whatever conditions it may deem necessary.		

International Cooperation		
International Best Practice	National Legislation	Comments
6. The State Party from which assistance is requested shall commit itself to inform the requesting State Party of the result of the implementation of the request. If the request is refused or postponed, the reasons of such refusal or postponement shall be given. The State Party from which assistance is requested shall inform the requesting State Party of the reasons that prevent the complete fulfilment of the request or the reasons for its considerable postponement. 7. The State Party requesting assistance may request the State Party from which assistance is requested to maintain the confidentiality of the nature and content of any request covered by this chapter, except in as far as necessary to implement the request. If the State Party from which assistance is requested cannot abide by this request concerning confidentiality, it shall so inform the requesting State Party which will then decide about the possibility of implementing the request. 8. a. In case of emergency, mutual assistance requests may be sent directly to the judicial authorities in the State Party from which assistance is requested from their counterparts in the requesting State Party. In such case, a copy shall be sent concurrently from the central authority in the requesting State Party to its counterpart in the State Party from which assistance is requested.		

International Cooperation		
International Best Practice	National Legislation	Comments
b. Communications can be made and requests submitted pursuant to this paragraph through INTERPOL. c. c.paragraph a, a request is submitted to an authority, but that authority is not competent to deal with that request, it shall refer the request to the competent authority and directly inform the requesting State Party accordingly. d. Communications and requests carried out according to this paragraph and not concerning compulsory procedures may be transmitted directly by the competent authorities in the requesting State Party to their counterpart in the State Party from which assistance is requested. e. Every State Party may, at the time of signature, ratification, acceptance or adoption, inform the General Secretariat of the Council of Arab Interior Ministers and the Technical Secretariat of the Arab Justice Ministers that requests according to this paragraph must be submitted to the central authority for reasons of efficiency.		

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
Article 26 BC **Spontaneous Information** 1. A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter. 2. Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.		**Legal Analysis** This is an important procedure to enable a state privy to information that will assist another state to prevent a cybercrime or to investigate it. Albeit available between CITO ratified states in CITO Article 33, Tunisia has no domestic legal basis to share such information with non-CITO states unless an official request is sent through the usual MLA channels. Article 18(4)-(5) UNTOC provides for the sharing of intelligence spontaneously for matters fulfilling the definition of a serious crime[438], that is transnational[439] and involves an organized crime group[440]. Without satisfying this definition an official request will need to be sent through the usual MLA channels to non-CITO states. On the basis of the fast-moving nature of cybercriminality spontaneous sharing is an effective way to cooperate with other states and its absence inhibits effective international collaboration with non-CITO states. **Gap Analysis** **Recommendation:** Use UNTOC Article 18(4)-(5) as the basis to spontaneously share information that fulfils the scope of UNTOC (with guarantees provided about use in evidence or disclosure of sensitive information to a third party (including another state).[441] Consider legislation based on Article 33 CITO or Article 26 BC.

[438] Article 2(b) UNTOC ““*Serious crime” shall mean conduct constituting an offence punish- able by a maximum deprivation of liberty of at least four years or a more serious penalty*”

[439] Article 3(1) UNTOC

[440] Article 2(a) UNTOC ““*Organized criminal group” shall mean a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit*”

[441] See Article 33(2) CITO

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
Article 33 CITO - Circumstantial Information 1. A State Party may – within the confines of its domestic law – and without prior request, give another State information it obtained through its investigations if it considers that the disclosure of such information could help the receiving State Party in investigating offences set forth in this convention or could lead to a request for cooperation from that State Party. 2. Before giving such information, the State Party providing it may request that the confidentiality of the information be kept; if the receiving State Party cannot abide by this request, it shall so inform the State Party providing the information which will then decide about the possibility of providing the information. If the receiving State Party accepts the information on condition of confidentiality, the information shall remain between the two sides.	**No equivalent**	
Article 32 BC **Trans-border access to stored computer data with consent or where publicly available** A Party may, without the authorisation of another Party: a. access publicly available (open source) stored computer data, regardless of where the data is located geographically; or b. access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.	**No equivalent**	**Legal Analysis** This procedural power enables a State to secure content stored in another state in limited circumstances. Article 32.b BC and Article 40 CITO is an exception to the principle of territoriality and permits unilateral trans-border access without the need for mutual legal assistance where there is consent or the information is publicly available. Examples of use of this procedural power under BC Article 32.b include: A person's e-mail may be stored in another State by a service provider, or a person may intentionally store data in another country. These persons may retrieve the data and, provided that they have the lawful authority, they may voluntarily disclose the data to law enforcement officials or permit such officials to access the data[442]

[442] Paragraph 294, page 53 BC Explanatory Report

International Cooperation		
International Best Practice	**National Legislation**	**Comments**
Section 27 HIPCAR – Forensic Software 1. If a [judge] [magistrate] is satisfied on the basis of [information on oath] [affidavit] that in an investigation concerning an offence listed in paragraph 7 herein below there are reasonable grounds to believe that essential evidence cannot be collected by applying other instruments listed in Part IV but is reasonably required for the purposes of a criminal investigation, the [judge] [magistrate] [may] [shall] on application authorize a [law enforcement] [police] officer to utilize a remote forensic software with the specific task required for the investigation and install it on the suspect's computer system in order to collect the relevant evidence. The application needs to contain the following information: • suspect of the offence, if possible with name and address; and • description of the targeted computer system; and • description of the intended measure, extent and duration of the utilization; • reasons for the necessity of the utilization. 2. Within such investigation it is necessary to ensure that modifications to the computer system of the suspect are limited to those essential for the investigation and that any changes if possible can be undone after the end of the investigation. During the investigation necessary to log		or A suspected terrorist is lawfully arrested while his/her mailbox – possibly with evidence of a crime – is open on his/her tablet, smartphone or other device. If the suspect voluntarily consents that the police access the account and if the police are sure that the data of the mailbox is located in another State, police may access the data under Article 32.b. **Gap Analysis** **Recommendation:** This restricted power to unilaterally secure evidence is included in legislation with safeguards to ensure the consent is lawfully obtained from the user.[443] Language can be used from Article 32 BC and Article 40 CITO. Article 32.b has been heavily criticized and it may be considered that the consent of the state where the stored computer data is stored is obtained in addition to the user. Section 27 HIPCAR provides for forensic software and this may allow access to a computer in another state. There are a number of restrictions that requires the evidence cannot be obtained by other means, a judicial order is required, can only apply to certain offences and is for a restricted period (3 months). Consideration should also be given *to consent of the other state where the forensic software may intrude.*

[443] Consideration should be given to situations such as the non-availability of a user (e.g. death) and if consent can be obtained in another state

International Cooperation		
International Best Practice	National Legislation	Comments
• the technical mean used and time and date of the application; and • the identification of the computer system and details of the modifications undertaken within the investigation; • any information obtained. Information obtained by the use of such software needs to be protected against any modification, unauthorized deletion and access. 3. The duration of authorization in section 27 (1) is limited to [3 months]. If the conditions of the authorization is no longer met, the action taken are to stop immediately. 4. The authorization to install the software includes remotely accessing the suspects computer system. 5. If the installation process requires physical access to a place the requirements of section 20 need to be fulfilled. 6. If necessary a [law enforcement] [police] officer may pursuant to the order of court granted in (1) above request that the court order an internet service provider to support the installation process. 7. [List of offences]. 8. A country may decide not to implement section 27. **Article 40 CITO - Access to Information Technology Information Across Borders** A State Party may, without obtaining an authorization from another State Party: 1. Access information technology information available to the public (open source), regardless of the geographical location of the information.		

International Cooperation		
International Best Practice	National Legislation	Comments
2. Access or receive – through information technology in its territory – information technology information found in the other State Party, provided it has obtained the voluntary and legal agreement of the person having the legal authority to disclose information to that State Party by means of the said information technology.		

Conclusion

The above legal and gap analysis show that the SPCs need to adapt and update their legislation to enable effective investigations and to ensure their national law can respond to cybercime threats. The legislative process can be slow and this increases the threat and harm caused by cybercrime. The priority is to legislate for those offences where there is no other possible offence in the national legislation and to ensure law enforcement have the tools required to effectively investigate perpetrators. The BC, HIPCAR and CITO should be used to draft and amend legislation to provide consistent application across the SPCs and allow for reciprocal use by the EU Member States. This will enable expeditious preservation and real-time collection of content and traffic data. As an immediate priority, 24/7 SPOCs should be established, to ensure international cooperation is effective and proactive.

The key recommendations from the gap analysis are as follows:

1. **It is recommended** that where the SPCs are yet to do so they are encouraged to sign, ratify and implement the Budapest Convention and/or CITO to enable MLA requests for real-time collection of traffic data, interception of content, production orders and spontaneous exchange of information.
2. **It is recommended** that SPOCs are designated by each SPC to process urgent outgoing and incoming MLA requests and remain updated on the processes to secure CSP data through both formal and informal means.
3. **It is highly recommended** that processes should be in place to preserve data to enable a MLA request to be sent – without preservation - data will be deleted and a MLA request cannot be executed

Annex A

Tunisian Statistics on Letters of Request

Origin of letters of request received By the Tunisian Technical Agency for Telecommunications during the period from 16 April 2014 to 10 June 2017	
Type	**Number**
National Guard Intelligence and Investigation Branch	836
National Police Centers	1372
Directorate of Judicial Police	454
Auxiliary branch of criminal cases	271
Justice	223
Directorate of Social Welfare	65
Auxiliary Directorate for Economic and Financial Investigation and Research	43
National Crime Research Unit for Terrorist crimes	204
Others	42
Total	**3510**

Subjects relating to letters of request received by the Tunisian Telecommunications Techniques Agency during the period from 16 April 2014 to 10 June 2017	
Facebook owner login	1290
Identifying the user of a mobile phone	1731
Identifying the identity of a computer thief	193
Identifying an exploiter of an IP address	107
Identifying a Skype account owner	7
Identification of the owner of an e-mail account	70
Identifying the owner of a website	51
Twitter account owner login	16
Identification of the owner of a YouTube account	2
Extracting content from a mobile phone or a computer	26
Divers	17
Total	**3510**

Bibliography

1. African Union, Oliver Tambo Declaration, Johannesburg 2009
2. African Union Convention on Cyber Security and Personal Data Protection
3. Arab League Convention on Combating Information Technology Offences
4. Budapest Convention on Cybercrime of the Council of Europe
5. Andy Greenberg (20 April 2011) Crypto Currency
6. Andy Greenberg (19 November 2014) Hacker Lexicon: What is the dark web?
7. Arab Social Media Report 2017 Debbie Stephenson (27 July 2014) Spear Phishing: Who's Getting Caught?
8. Comparative Analysis of the Malabo Convention of the African Union and the Budapest Convention on Cybercrime 20 November 2016
9. Eric Tamarkin, (20 January 2015) The AU's Cybercrime Response. A Positive Start, but Substantial Challenges Ahead, Policy Brief 73
10. Explanatory Report Budapest Convention (185) No.10
11. Explanatory Report to the Convention on Cybercrime, No. 298.
12. Gercke, 10 Years Convention on Cybercrime, Computer Law Review International, 2011
13. ICMEC Model Legislation and Global Review 8th EditionITU Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report, 2008
14. Strategic Seminar "Keys to Cyberspace" Eur ojust, The Hague, 2 June 2016 Outcome Report
15. Lange/Nimsger (2004) Electronic Evidence and Discovery and Whitcomb, An Historical Perspective of Digital Evidence: A Forensic Scientist's View, International Journal of Digital Evidence, 2002, Vol. 1, No. 1.
16. Mohamed N. El-Guindy (2012) Cybercrime Challenges in the Middle East
17. Mohamed N. El-Guindy (2014) Middle East Security Threat Report
18. R. Moore (2005) Cyber crime: Investigating High-Technology Computer Crime
19. Ramzan, Zulfikar (2010) Phishing attacks and countermeasures - In Stamp, Mark & Stavroulakis, Peter Handbook of Information and Communication Security Springer.
20. T-CY Guidance Notes – 1 March 2017
21. The Enhacing Competitiveness in the Caribbean through the Harmonization of ICT Policies Legislation and Regulatory Procedures
22. Tor Project: FAQ
23. Verdelho (2008) The effectiveness of international cooperation against cybercrime
24. Warren G. Kruse, Jay G. Heiser (2002) Computer forensics: incident response essentials
25. ACKNOWLEDGEMENTS
26. Special thanks to the commitment and dedication of the scientific consultants whose contribution was essential to the production of this paper.

PORTADA INDEX