Proposed Amendments to Align Computer Misuse and Cybercrime Act (CMCA) 2003 with Budapest Convention on Cybercrime and AU Convention on Cybersecurity and Personal Data Protection

CERT-MU Team, National Computer Board
Ministry of Technology, Communication and Innovation

Why Need to Review CMCA 2003

To make it an adequate and efficient piece of legislation on cybercrime and electronic evidence that allows proper prosecution and adjudication of cases related to cybercrime.

Review Process

- Mauritius is a party to the GLACY+ Project of the Council of Europe (CoE) since 2013
- The project is focused on building capacity of member countries on cybercrime
- Under the GLACY+ Project, CoE is providing assistance for the harmonisation of domestic laws with the Budapest Convention on Cybercrime.
- CoE conducted a National Assessment Meeting in Port Louis from 22 to 24 January 2018 to review the CMCA 2003. Various stakeholders attended the meeting.

Scope of the Review Process

1. CMCA Existing Provisions (Section 2-22)
2. Provisions of Budapest Convention to be integrated in CMCA (Article 1-48)
3. Provisions of AU Convention on Cybersecurity and Personal Data Protection (Article 1-38)
4. Integration of new provision to provide legal mandate to CERT-MU
5. Integration of new provision on Cyber Threat Monitoring
6. Integration of new provision on Critical Information Infrastructure Protection (CIIP)

Gaps Identified in CMCA 2003 (1)

Section 3 of the CMCA criminalizes unauthorized access to computer data. Subsection (4) refers to "program or data" though the actual offence under subsection (1) only appears to apply to computer systems and not specifically to programs. Thus, it is unclear whether access to a computer program is criminalized. Further subsection (2) provides certain exceptions to liability, whereas subsection (3) provides overlapping criteria when conduct is not authorised. The use of two separate exclusionary criteria results in ambiguity in determining what conduct is legal. Section 4, which relates to access with the intent to commit other offences, does not include the word "unauthorized" and thus criminalizes authorized conduct.

Gaps Identified in CMCA 2003 (2)

Section 5 of the CMCA criminalizes unauthorized interception. Under this section, access to a computer system is pre-requisite conduct for the offence of unauthorized interception. Section 5 does not criminalize the interception of transmissions of computer data to, from and within a computer system. Moreover, the definition of "intercept" under Section 2 of the CMCA is overly broad and extends to non-technical interception.

Gaps Identified in CMCA 2003 (3)

Section 6 of the CMCA criminalizes data interference. This provision does not appear to criminalize the deterioration and suppression of computer data.

Section 7 of the CMCA criminalizes system interference, though the scope of this offence appears to be limited to DDOS attacks and technical failures in computer systems, rather than serious hindrance by technical means. Moreover, it is unclear what is meant by "without lawful authority or without lawful excuse".

Gaps Identified in CMCA 2003 (4)

There is no provision in the CMCA corresponding to Article 7 of the Budapest Convention (computer-related forgery) and though the provision for traditional forgery under the Criminal Code extends to forgery of documents in electronic form, the Criminal Code does not provide any specific language regarding rendering data inauthentic and thus does not encapsulate the offence of computer-related forgery

Gaps Identified in CMCA 2003 (5)

The Child Protection Act criminalizes the production, distribution, possession or publication of indecent photographs and pseudo-photographs. Though the term "photograph" includes data stored by electronic means, it requires that such data must be capable of conversion to a photograph. Similarly, "pseudo-photograph" may include computer graphics though these must appear to be photographs

Gaps Identified in CMCA 2003 (6)

The Copyright Act 2014 criminalizes the reproduction of work through electronic means for commercial purposes. However, given that the definition of "distribution to the public" is limited to distribution in tangible form, the Copyright Act 2014 does not criminalize distribution of work through electronic means.

Gaps Identified in CMCA 2003 (7)

The Copyright Act 2014 criminalizes the reproduction of work through electronic means for commercial purposes. However, given that the definition of "distribution to the public" is limited to distribution in tangible form, the Copyright Act 2014 does not criminalize distribution of work through electronic means.

Gaps Identified in CMCA 2003 (8)

Part III of the CMCA provides most of the procedural and investigative powers required by the Budapest Convention. With respect to the scope of the powers related to preservation orders (Section 11) and disclosure of preserved data (Section 12), it is unclear whether these powers may be exercised with respect to offences under the CMCA or generally with respect to investigation of any offence involving evidence in electronic form. Production orders (Section 13) and powers of access, search and seizure (Section 14) may be exercised with respect to any offence. However, real-time collection of traffic data (Section 15) may only be exercised with respect to offences under the CMCA.

Gaps Identified in CMCA 2003 (9)

Section 11 which provides for preservation orders extends beyond stored computer data to data processed by means of a computer system, though it is unclear how this power may be exercised with respect to data that is no longer stored in a computer system. Moreover, this exceeds the scope of the Budapest Convention as it enables preservation of subscriber information. This provision does not specify any fixed time period, which renders it inconsistent with the 90-day preservation limit under Article 16 of the Budapest Convention. Section 12 which relates to disclosure of preserved data also exceeds the scope of the Budapest Convention and is in effect a production order power as it relates to all data and not only preserved traffic data

Gaps Identified in CMCA 2003 (10)

The power to order production of data under Section 13 of the CMCA is largely consistent with the Budapest Convention. Similarly the powers of access, search and seizure under Section 14 of the CMCA are largely consistent with the Budapest Convention, though given that the search warrant must relate to a specific premises, this may not enable searching or similarly accessing data stored virtually. Section 14 also does not enable law enforcement to extend the scope of a search and seizure to other computer systems.

Section 15 of the CMCA which relates to real-time collection of traffic data is largely consistent with the Budapest Convention, though it may only be exercised with respect to offences under the CMCA and not generally as part of investigation of any offence involving evidence in electronic form.

Gaps Identified in CMCA 2003 (11)

There is no specific provision enabling the interception of content data under the CMCA. Section 32 of the Electronic Transactions Act enables the interception of communications by operators without any prior order or supervision from an independent authority if it has reason to believe the message is indecent or abusive, in contravention of the Act or likely to endanger or compromise defence, public safety or public order. This does not enable interception of specified communications in relation to an investigation of serious offences.

Recommendations

1. Align and harmonise the use and the scope of use of the terms *"electronic evidence/record/digital record/information in electronic form or electronic document"*.
2. Insert the offence of computer-related forgery into the Computer Misuse and Cybercrime Act.
3. Consider amending the Computer Misuse and Cybercrime Act to provide for aggravated offences on the confidentiality, integrity and availability of critical infrastructure.
4. Amend and clarify the scope of the investigative powers and procedures in the Computer Misuse and Cybercrime Act to ensure their applicability to any criminal investigation of any criminal offence and not only offences under the Computer Misuse and Cybercrime Act.

Recommendations (contd)

5. Consider amending the procedural powers related to preservation orders and disclosure of preserved data to align with the expeditious powers provided under the Budapest Convention.
6. Consider inserting a specific procedural power enabling the interception of content data of specified communications in real-time in relation to serious offences.
7. Consider amending the Computer Misuse and Cybercrime Act to provide legal cover and mandate to the CERT-MU and provisions on CIIP.

Recommendations (contd)

8. To implement mechanisms legally binding and enforceable under domestic law governing the receiving and sending of request of mutual legal assistance and international cooperation based upon and consistent with the Budapest Convention and to enable specialized international cooperation powers such as mutual assistance regarding accessing of stored computer data, trans-border access to stored computer data with consent or where publicly available, mutual assistance regarding the real-time collection of traffic data or mutual assistance regarding interception of content data.

Recommendations (contd)

9. Consider establishment or designation of a 24/7 Network that would enable immediate mutual assistance in the provision of technical advice, preservation of data, collection of evidence, provision of legal information and locating of suspects.

Sections to be Amended in CMCA 2003

- Section 2- Interpretation
- Section 3- Unauthorised access to computer data
- Section 5-Unauthorised access to and interception of computer service
- Section 6- Unauthorised modification of computer material
- Section 7- Damaging or denying access to computer system
- Section 8-Unauthorised disclosure of password
- Section 9-Unlawful possession of devices and data
- Section 10-Electronic Fraud
- Section 11-Preservation Order
- Section 12, 13 and 14, 12-Disclosure of Preserved Data, 13-Production Order, 14- Powers of Access, Search and Seizure
- Section 15-Indecent Photograph of children

New Provisions to be in line with the Budapest Convention

1. General principles relating to international co-operation (Article 23);
2. Extradition (Article 24);
3. General principles relating to mutual assistance (Article 25);
4. Spontaneous information (Article 26);
5. Procedures pertaining to mutual assistance requests in the absence of applicable international agreements (Article 27);
6. Confidentiality and limitation on use (Article 28);
7. Expedited preservation of stored computer data (Article 29);

New Provisions to be in line with the Budapest Convention

8. Expedited disclosure of preserved traffic data (Article 30)
9. Mutual assistance regarding accessing of stored computer data (Article 31)
10. Trans-border access to stored computer data with consent or where publicly available (Article 32);
11. Mutual assistance regarding the real-time collection of traffic data(Article33)
12. Mutual assistance regarding the interception of content data (Article 34)
13. 24/7 Network (Article 35)
14. New provision relating to the input, alteration, deletion, or suppression of computer data

Additional Provisions

15. AU Convention on Cybersecurity and Personal Data Protection

16. Provisions on to provide legal mandate to CERT-MU

17. Provisions on the CIIP

Details on the Amendments….

Thank You for your Attention