HIPSSA Project

QUESTIONNAIRE
CYBERCRIME LAW - ZIMBABWE[1]

[1] **The following Questionnaire pertains to the description of cybercrime law in your country. These laws are enacted to safeguard and protect the use of cyberspace in communicating and transacting. The law may be a single designated legislation or, alternatively anti-cybercrime provisions may appear in electronic commerce legislation, consumer protection legislation, telecommunications legislation. Some countries have dedicated structures to enforce cybercrime laws, and for incidence detection, prevention and management. Cybercrime laws may or may not result from cybercrime policy in a country.**

QUESTIONAIRE

CYBERCRIME LEGISLATION QUESTIONS

Name:

Organisation:

Title:

1. Does your country have a current Policy on cybercrime?

   Yes ___ No ___

   If yes, please list and attach copies of all such policy documents, preferably in electronic format if possible.

   If No, please set the reasons why there is not a policy on cybercrime in your country?

   _____

2. Does cybercrime have a designated legislation or it is covered by general legislation?

   Please list and attach copies of all such legislation, preferably in electronic format if possible.

3. In which of the following areas does your country have existing cybercrime legislation in place?

   a. Substantive cybercrime laws

Illegal access to a computer system

Illegal access (to a computer system) refers to acts where the offender enters parts or the whole of a computer system without authorisation or justification. This is for example the case if the offender circumvents a firewall and breaks into the computer system of a bank. The term computer

system may be interpreted in a broad manner and also include smart phones, wireless router and external storage devices.

Yes ___ No ___

If yes, please list and attach copies of all such legislation, preferably in electronic format if possible:

- **Illegal data acquisition of computer data**
  Illegal acquisition of computer data refers to acts where the offender obtained computer data (e.g. by copying them) without authorization. This is for example the case if the offender, who is working for a company, without authorization, copies files to take them with him.

Yes ___ No ___

If yes, please list and attach copies of all such legislation, preferably in electronic format if possible:

- **Illegal interception of data**
  Illegal interception of computer data refers to acts where the offender is obtaining computer data during a – in general non-public - transmission process. This is for example the case if the offender is recording transmissions within a wireless network.

Yes ___ No ___

If yes, please list and attach copies of all such legislation, preferably in electronic format if possible:

- **Illegal data interference**
  Illegal data interference refers to acts where the offender interferes with stored computer data – e.g. by deleting, suppressing or modifying them. This is for example the case if malicious software changes the configuration of a computer system to prevent an identification of the presents of such software by an anti-virus solution or deletes files on the affected computer system.

Yes ___ No ___

If yes, please list and attach copies of all such legislation, preferably in electronic format if possible:

- **Illegal system interference**
  Illegal system interference refers to acts where the offender is hindering the functioning of a computer system. This is for example the case if the offender is submitting so many requests to a computer system that it can't respond to legitimate requests anymore (so called "denial-of-service attack").
  Yes ___ No ___

  If yes, please list and attach copies of all such legislation, preferably in electronic format if possible:

- **Production/Distribution of tools to commit computer crime**
  Production, distribution, possession, etc. of illegal computer tools refers to acts, where the offender develops or distributes hard- or software solutions that can be used to carry out computer or Internet-related offences. This is for example the case if the offender develops a software to automate denial-of-service attacks.

  Yes ___ No ___

  If yes, please list and attach copies of all such legislation, preferably in electronic format if possible:

- **Fraud and computer-related fraud**
  Computer-related fraud refers to an interference with computer- or data processing processes with the intent of procuring an economic benefit. This is for example the case if the offender modifies a software used by a bank to redirect money transfer processes to his own account.

  Yes ___ No ___

  If yes, please list and attach copies of all such legislation, preferably in electronic format if possible:

- **Falsification of documents, computer-related forgery**
  Computer-related forgery refers to acts where the offender interferes with computer data – that are used for legal purposes - in a way, that they result in inauthentic data. This is for example the case if the offender modifies an authentic mail from a financial institution and sends it out to various recipients.

Yes ___ No ___

If yes, please list and attach copies of all such legislation, preferably in electronic format if possible:

- **Identity-related crime**
  Identity-related crime refers to acts where the offender transfers, possesses or uses means of identification of another person with the intent to commit, aid or abet any unlawful criminal activity. This is for example the case if an offender, who obtains credit card information from a victims computer system sells such data or uses it to mislead investigations while committing a crime.

Yes ___ No ___

If yes, please list and attach copies of all such legislation, preferably in electronic format if possible:

- **Child pornography**
  Computer-related production, distribution, possession, etc. of child abuse material refers to acts where the offender produces/interacts with electronically stored child abuse material. This is for example the case if an offender downloads a digital picture showing the sexual abuse of a child.

Yes ___ No ___

If yes, please list and attach copies of all such legislation, preferably in electronic format if possible:

- **SPAM**
  Sending of SPAM refers to acts where an offender is sending out messages to a large number of recipients without authorization or request.

Yes ___ No ___

If yes, please list and attach copies of all such legislation, preferably in electronic format if possible:

- **Offences related to an investigation**
  Crimes safeguarding investigations refers to acts where the offender interferes with an investigation by violating certain safeguards. This can for example be the case if a provider was requested to keep confidential

that he received an order to intercept the communication of a suspect but he informs the suspects about this issue.

Yes ___ No ___

If yes, please list and attach copies of all such legislation, preferably in electronic format if possible.

b. Substantive criminal law

- Do you believe that any of the above offences should NOT be criminalized? If you believe that one or more offences should not be criminalized, please specify if they should not be criminalized at all or if the criminalization should be restricted:

c. Procedural cybercrime law/s for example

- authority to preserve and obtain electronic data from third parties, including internet service providers;

Yes ___ No ___

If yes, please list and attach copies of all such legislation, preferably in electronic format if possible:

- authority to intercept electronic communications;

Yes ___ No ___

If yes, please list and attach copies of all such legislation, preferably in electronic format if possible:

- authority to search and seize electronic evidence,

Yes ___ No ___

If yes, please list and attach copies of all such legislation, preferably in electronic format if possible:

- seizing computer systems and equipment

Yes ___ No ___

If yes, please list and attach copies of all such legislation, preferably in electronic format if possible:

d. Procedural instrument

- The successful investigation of crimes requires that law enforcement agencies have the ability to use specific investigation instruments. Do you believe that law enforcement should NOT have the ability to use any of the following instruments? If you believe that one of more instruments should not be available please specify if they should NOT be available at all or if the application should be restricted (e.g. to specific offences):
    - Activating a computer system of a suspect
    - Searching for data on the suspects computer and storage devices
    - Seizing computer systems and equipment
    - Instead of seizing the hardware making copies of relevant data
    - Ordering somebody who is not the suspect but has special knowledge about the functioning of a computer system or the location of specific data (such as a system administrator) to support the investigation
    - Interception of content data of a suspect (such as e-mails)
    - Recording traffic data of the suspect (such as the address of a website that the suspects visits)
    - Using advanced remote forensic tools (such as keyloggers)

c. International Cooperation and Mutual legal assistance related to cyber-crime:

Yes ___ No ___

If yes, please list and attach copies of all such legislation, preferably in electronic format if possible:

_____

_____

4. a. What are the top 3 or top 5 Cybercrime offenses that your country suffers from most?

b. What are the main problems with regard to a successful investigation/prosecution of Cybercrime in your country.

c. Please identify whether the following forms of cybercrime (1) occur frequently, (2) occur infrequently, or (3) have not occurred, by placing an "X" as appropriate in the following table:

Forms of Cybercrime	Occur Frequently	Occur Infrequently	Has not Occurred
Online identity theft (including phishing and online trafficking in false identity information)			
Hacking (illegal intrusion into computer systems; theft of information from computer systems)			
Malicious code (worms, viruses, malware and spyware)			
Illegal interception of computer data			
Online commission of intellectual property crimes			
Online trafficking in child pornography			
Intentional damage to computer systems or data			
Data Espionage			

Illegal Data Interference			
Illegal System Interference			
Illegal Devices			
Computer-related Forgery			
Computer-related Fraud			
SPAM			

b. In addition, to the above, if there are there any other forms of cybercrime that have occurred, please identify them as well as the frequency with which they occur in the following table.

Other cybercrime Conduct	Occur Frequently	Occur Infrequently

5. Does your country have any concrete experiences with respect to strengthening the relationship between the authorities responsible for investigating and/or prosecuting cyber-crimes, and internet service providers that may be shared with other States as a best practice in this area?

Yes ___ No ___

If yes, please explain:

6. Has your country identified, created, or established a unit or entity specifically charged with dealing cyber-crimes incident response (e.g. CERT)?

Yes ____ No ___

If yes, please provide the following information:

i. The exact name of the unit/entity:

ii. The institution to which the unit/entity belongs:

iii. The number of officers or experts in the unit/entity:

iv. The regional and international organizations that unit/entity collaborate with:

7. Has your country identified, created, or established a unit or entity specifically charged with directing and developing the investigation of cyber-crimes?

Yes ___ No ___

If yes, please provide the following information:

_____

i. The exact name of the unit/entity:

ii. The institution to which the unit/entity belongs:

iii. The number of officers or investigators in the unit/entity:
iv. The regional and international organizations that unit/entity collaborate with:

If such a unit/entity has been created or established, are its functions dedicated exclusively to the investigation of cyber-crimes?

Yes ___ No ___

If no, what other types of offenses or crimes is this unit/entity responsible for investigating and/or prosecuting?

_____
_____

8. Has your country identified, created, or established a unit or entity specifically charged with directing and the prosecution of cyber-crimes?

Yes ___ No ___

If yes, please provide the following information:

_____
_____

v. The exact name of the unit/entity:
_____

vi. The institution to which the unit/entity belongs:
_____

vii. The number of prosecutors or judicial officials in the unit/entity:
_____

v. The regional and international organizations that unit/entity collaborate with:

_____

If such a unit/entity has been created or established, are its functions dedicated exclusively to the prosecution of cyber-crimes?

Yes ___ No ___

If no, what other types of offenses or crimes is this unit/entity responsible for prosecuting?

_____

_____

9. Has your country identified, created, or established a specific court for the trials of cybercrimes?

Yes ___ No ___

If yes, please provide the following information:

_____

_____

vi. The exact name of the court:

_____

vii. The institution to which the court belongs:

_____

viii. The number of judges and experts in the court:

_____

ix. The regional and international organizations that court collaborates with:

_____

If such a court has been created or established, are its functions dedicated exclusively to the trials of cybercrimes?

Yes ___ No ___

If no, what other types of offenses or crimes is this court responsible for trying?

_____

_____

10. Are there any challenges (legal, technical and institutional) faced by your country in developing frameworks for cybercrime and critical information infrastructure protection (CIIP)?

    Yes __ No ___

    If yes, please identify them.

11. are there any barriers and constraints (legal, technical and institutional) in your country that affect the development of cybercrime legislation framework and critical information infrastructure protection (CIIP) for tackling cybercrime?

    Yes ___ No ___

    If yes, please identify them.

Does your country receive updated information on development activities being undertaken by regional and international organizations in respect of cybercrime? Please specify the names of such organizations.