Cybercrime Act, 2007

In implementation of the Interim Constitution of the Republic of Sudan of the year 2005, the National Council has endorsed and the President of the Republic has signed the Act the text of which is below.

Chapter One

Preliminary provisions

Name of the law and entry into force

1. This law shall be called the Cybercrime Act, 2007, and shall enter into force on the date of its [publication].

Application

2. The provisions of this Act shall apply to all of the offences provided for herein if they have been committed wholly or in part in or outside Sudan or if their impact has extended to Sudan, whether the original perpetrator, accomplice or instigator of those offences is punishable outside Sudan, taking into account the general principles enshrined in the Criminal Code of the year 1991.

Definitions

3. In this Act, unless the context requires otherwise:

"cyber"	shall mean information systems, networks and communications, software, computers, the Internet and related activities.
"data and information"	shall mean numbers, letters and symbols, and everything that they are able to store, process, generate, produce and transfer to a computer or other electronic medium.
"information system"	shall mean all software, tools and equipment for the production, storage or processing of data or information or management of data or information.
"information network"	shall mean any connection between more than one information system in order to obtain or exchange information.
"site"	shall mean a place where information is available on an information network through a specific address.
"capture"	shall mean showing, hearing or obtaining any data or information contained in any electronic message.
"information media"	shall mean information technology and communications devices.
"content"	shall mean the content of electronic material whether that content is text, image, sound or video or similar.

Chapter Two

Information system, media and network offences

Accessing sites and information systems owned by others

4. Anyone who accesses a site or information system without being authorized to do so and:

   (a) consults or copies it, shall be liable to imprisonment for a period not exceeding two years or a fine or both penalties;

   (b) cancels data or information belonging to another person or deletes, destroys, discloses, damages, alters or republishes it or who changes the design or location of the site or cancels or diverts its address shall be punishable by imprisonment for a period not exceeding four years or a fine or both penalties.

Access of sites and information systems by a public official

5. Any public employee who without authorization accesses a site or information system of the authority in which he works or who facilitates another person's doing so shall be punishable by a prison sentence not exceeding five years or a fine or both penalties.

Tapping, interception or capture of messages

6. Any person who taps, captures or intercepts any message through an information network or computer hardware or similar without permission from the public prosecutor or the competent authority or the party to which the information belongs shall be liable to a term of imprisonment not exceeding three years or a fine or both penalties.

The offence of accessing sites deliberately in order to obtain secure data or information

7. Any person who deliberately accesses a site or system directly or through an information network or similar for the purpose of:

   (a) obtaining data or information affecting the national security of the country or the national economy shall be liable to a prison sentence not exceeding seven years or a fine or both penalties;

   (b) cancels, deletes, destroys or alters information affecting the national security of the country or the national economy shall be liable to a prison sentence not exceeding ten years or a fine or both penalties.

Shutting down, disabling or destroying software, data or information

8. Any person who accesses by any means whatsoever an information system, medium, network or similar and deliberately shuts it down or disables it or destroys, erases, deletes or damages software, data or information shall be liable to a prison sentence not exceeding six years or a fine or both penalties.

Obstruction of, interference with, or disabling access to the service

9. Any person who intentionally obstructs, interferes with or disables by any means whatsoever access to the service or access to hardware, software or sources of data or information through an

information network or computer hardware or similar shall be liable to a prison sentence not exceeding two years or a fine or both penalties.

Chapter three

Crimes against property, data and communications by threats or blackmail

10. Any person who uses an information network or computer hardware or similar to threaten or blackmail another person in order to induce them to perform or not to perform an act even if that act or omission is lawful shall be liable to a prison sentence not exceeding two years or a fine or both penalties.

Fraud or impersonation

11. Any person who communicates through an information network or computer hardware or similar by fraud or using a false name or impersonation for the purpose of himself or another person taking possession of money or a bond or a signature of a bond shall be liable to a prison sentence not exceeding four years or a fine or both penalties.

Obtaining credit card numbers or data

12. Any person who uses an information network or computer hardware or similar to obtain credit card numbers or data or similar for the purpose of using them to obtain the money or data of another person or the services that result from those data or numbers shall be liable to a prison sentence not exceeding five years or a fine or both penalties.

Unlawful use of communications services

13. Any person who benefits unlawfully from communications services through an information network or computer hardware or similar shall be liable to a prison sentence not exceeding four years or a fine or both penalties.

Chapter four

Public order and morality offences

Breach of public order and morality

14. (1) Any person who produces, prepares, creates, sends, stores or disseminates through an information network, computer hardware or similar any content breaching decency, public order or morality shall be liable to a prison sentence not exceeding five years or a fine or both penalties.

(2) Any person who intentionally or though negligence provides or facilitates through an information network, computer hardware or similar access to content breaching decency or contrary to public order or morality shall be liable to a prison sentence not exceeding five years or a fine or both penalties.

(3) If the act referred to in paragraphs (1) and (2) involves a juvenile, the offender shall be liable to a prison sentence not exceeding seven years or a fine or both penalties.

Creation or publication of sites with a view to disseminating ideas and programmes contrary to public order or morality

15. Any person who creates, publishes or uses a site on a cyber network, computer hardware or similar or who disseminates programmes or ideas that are contrary to public order or morality shall be liable to a prison sentence not exceeding three years or a fine or both penalties.

Violation of religious beliefs or the sanctity of private life

16. Any person who violates or abuses any religious belief or the sanctity of private life through an information network, computer hardware or similar shall be liable to a prison sentence not exceeding three years or a fine or both penalties.

Defamation

17. Any person who uses an information network, computer hardware or similar for the purpose of defamation shall be liable to a prison sentence not exceeding two years or a fine or both penalties.

Chapter five

Terrorism and intellectual property offences

Creation or publication of sites for terrorist groups

18. Any person who creates, publishes or uses a site on an information network, computer hardware or similar for a terrorist group under any name to facilitate communication by its leadership or its members or to disseminate its ideas or funding or how to manufacture incendiary or explosive materials or any device used in terrorist acts shall be liable to a prison sentence not exceeding seven years or a fine or both penalties.

Publication of intellectual works offences

19. Any person who publishes unlawfully through an information network, computer hardware or similar intellectual or literary works or scientific research or similar shall be liable to a prison sentence not exceeding one year or a fine or both penalties.

Chapter six

Trafficking in human beings and drugs, and money-laundering offences

Trafficking in human beings

20. Any person who creates or publishes a site on an information network, computer hardware or similar for the purposes of trafficking in human beings or facilitating such a transaction shall be liable to a prison sentence not exceeding ten years or a fine or both penalties.

Trafficking in or distributing drugs or narcotics

21. Any person who creates or publishes a site on an information network, computer hardware or similar for the purposes of trafficking in or distributing drugs or narcotics or similar or facilitating such a transaction shall be liable to a prison sentence not exceeding twenty years or a fine or both penalties.

Money-laundering

22. Any person conducting a money-laundering operation by facilitating, transferring, distributing or recycling money through a site on an information network, computer hardware or similar in order to obtain for it a legal character with the knowledge that it is derived from an unlawful source shall be liable to a prison sentence not exceeding ten years or a fine or both penalties.

Chapter seven

General provisions

Incitement, agreement or complicity

23. (1) Any person who incites, aids, agrees to or participates with others in the commission of one of the offences provided for in this Act shall be considered to have committed the offence of incitement, even if [the offence] has not been committed, and shall be liable to half the penalty prescribed for it.

(2) If the offence has been committed as a result of that incitement, the inciter shall be liable to the same penalty as that prescribed for the offence itself.

Instigation

24. Any person who has instigated the commission of one of the offences provided for in this Act shall be considered to have committed the offence of instigation and shall be liable to the penalty prescribed for it.

Confiscation

25. Without prejudice to the rights of bona fide third parties, the court shall in all cases order the confiscation of hardware, software or media used in the commission of any of the offences provided for in this Act and of the funds proceeding from them. The court shall also close the premises or enterprise in which any of the offences provided for in this Act have been committed, if the offence was committed with the knowledge of their owner, and shall do so for the period that it deems appropriate.

Deportation of foreigners

26. In addition to any penalties provided for in this Act or any other act and bearing in mind the provisions of international treaties, the court shall, where the offences provided for in articles 7, 15, 16, 18, 20, 21 and 22 have been committed, order deportation if the convicted person is a foreigner.

Chapter eight

Law enforcement procedures

Publication of rules

27. Without prejudice to the Criminal Procedures Act of 1991, the Chief Justice shall issue special rules determining the procedures to be followed in the prosecution of the offences provided for in this Act.

Special court

28. The Chief Justice shall, in accordance with the Judiciary Act 1986, establish a special court for the offences provided for in this Act.

Special prosecution service

29. Under the provisions of the Organization of the Ministry of Justice Act of 1983, a special prosecution service shall be established for cybercrime.

Special police force

30. Under the provisions of the Police Act of 1999, a special police force shall be established for cybercrime.

Certification

I hereby certify that the National Council endorsed the Cybercrime Act 2007 at sitting No. 2 of its fourth session on 30 May 2007, and that the Joint Standing Committee of the Two Councils decided at its meeting No. 10 on 3 June 2007 that this Act did not affect the welfare of the States.

Ahmed Ibrahim al-Tahir, President of the National Council, President of the Joint Standing Committee of the Two Councils

Approved, Field-Marshal Omar Hassan Ahmed al-Bashir, President of the Republic, 30.06.2007