77. Administrative penalties for contraventions

The Authority shall, for the purpose of imposing an administrative penalty under this Act, take into account;

(a) the size of the service provider concerned;
(b) the criticality of the sector;
(c) the impact of the contravention; and
(d) any other relevant criterion that the Competent Minister may determine.

78. Extradition

Any offence under this Act is an extraditable crime for which extradition may be granted or obtained under the applicable law for extradition.

79. Forfeiture

The Court before which a person is convicted of an offence may, in addition to any other penalty imposed, order the forfeiture of any apparatus, article or device which is the subject matter of the offence or is used in connection with the commission of the offence.

80. Regulations

The Competent Minister may issue regulations and guidelines necessary for effective implementation of this Act.

72. Hacking E-payment Devices

A person who intentionally accesses, tampers with, alters, manipulates, or interferes with any electronic payment device, including point-of-sale (POS) machines, mobile money terminals, ATMs, or any digital financial transaction system without authorization, commits an offence and upon conviction shall be liable to a fine or imprisonment for a term not exceeding seven years, or both.

CHAPTER VII
GENERAL PROVISIONS

73. Co-operation

A public institution or a private institution shall co-operate with the Authority for the purpose of ensuring the cybersecurity of the country.

74. General Penalty

A person who contravenes a section of this Act for which a penalty is not provided commits an offence and shall be liable upon conviction to a fine or imprisonment for a term not exceeding five years, or both.

75. Guidelines

The Authority shall publish guidelines that it considers necessary for;
(a) the identification of critical infrastructure;
(b) the registration of critical infrastructure;
(c) the protection of critical infrastructure;
(d) the management of critical infrastructure;
(e) access to, transfer and control of data in critical information infrastructure;
(f) the storage or archiving of data or information in critical infrastructure;
(g) reporting incidents involving critical infrastructure; and
(h) any other matter required for the adequate protection of critical infrastructure.

76. Directives

(1) The Authority may issue directives to an owner of a critical infrastructure, a cybersecurity service provider or service providers for the purpose of ensuring the cybersecurity of the country.
(2) An owner of a critical information infrastructure, a cybersecurity service provider or a service provider who fails to comply with the directives issued under subsection (1) of this section shall be liable to pay to the Authority the administrative penalty prescribed under this Act.

advantage received, whichever is greater, or imprisonment for a term not exceeding ten years, or both.

66. Computer-related forgery

(1) A person who, intentionally and without authorisation, 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 of whether or not the data is directly readable and intelligible, commits an offence and shall be liable upon conviction to a fine three times the value of undue advantage received, whichever is greater, or imprisonment for a term not exceeding ten years, or both.

(2) A person who performs the acts described under this subsection (1) of this section;

(a) for wrongful gain;

(b) for wrongful loss to another person; or

(c) for any benefit for oneself or for another person,

shall be liable upon conviction to a fine or imprisonment for a term not exceeding five years, or both.

67. Cyber Harassment

A person who intentionally uses a computer system, electronic communication, or any digital platform to threaten, insult, demean, or otherwise cause psychological distress, fear, or emotional harm to another person, commits an offence and upon conviction shall be liable to a fine or imprisonment for a term not exceeding five years, or both.

68. Hacking

A person who intentionally accesses or causes access to a computer system, computer program, data, or network without lawful authority or permission commits an offence and upon conviction shall be liable to a fine or imprisonment for a term not exceeding ten years, or both.

69. Cyberattack

A person who intentionally initiates, carries out, or attempts to carry out a cyberattack against a computer system, computer network, data, or critical information infrastructure, including through malware, viruses, denial-of-service attacks, ransomware, or any other harmful technological means, commits an offence and upon conviction shall be liable to a fine or imprisonment for a term not exceeding fifteen years, or both.

70. Hacking The Government Institutions Information Systems

A person who intentionally and without lawful authority accesses, attempts to access, interferes with, or causes any form of unauthorized intrusion into the information system, database, network, or digital infrastructure of any Government Institution of the Republic of South Sudan, commits an offence and upon conviction shall be liable to a fine or imprisonment for a term not exceeding twenty years. or both.

71. Creating Fake Emails, Websites and Electronic Accounts

A person who intentionally creates, registers, or operates a fake email address, website, social media account, or any other electronic account for the purpose of impersonation, deception, fraud, or misleading the public commits an offence and, upon conviction shall be liable to a fine or imprisonment for a term not exceeding five years, or both.

offence and upon conviction shall be liable to a fine or imprisonment for a term not exceeding ten years, or both.

60. Cyber Espionage

A person who uses a computer or computer system to conduct espionage activities commits an offence and shall be liable upon conviction to a fine or imprisonment for a term not exceeding twenty years, or both.

61. Economic Sabotage

A person who uses a computer or a computer system to engage in activities related to economic sabotage including, but not limited to, tax evasion, interference with revenue collection or its disbursement and money laundering commits an offence and upon conviction shall be liable to a fine or imprisonment for a term not exceeding seven years, or both.

62. Attempt, conspiracy, aiding and abetting

A person who;

(a) attempts to commit any offence under this Act; or aids, abets, conspires, counsels or procures another person(s) to commit any offence under this Act commits an offence and shall be liable upon conviction to the punishment provided for the principal offence under this Act;

(b) An employee of a financial institution found to have connived with another person or group of persons to perpetrate fraud using computer system(s) or network, commits an offence and shall be liable upon conviction to a fine or imprisonment for a term of not exceeding seven years and shall in addition, refund the stolen money or forfeit any property to which it has been converted to the bank, financial institution or the customer.

63. Spreading of computer virus

A person who, engages in malicious or deliberate spread of viruses or any malware thereby causing damage to critical information in public, private or financial institution's computers commits an offence and shall be liable upon conviction to a fine or imprisonment for a term not exceeding three years or both.

64. Use of fake profile

A person who, individually or with other persons, makes use of a fake profile to cause harm, commits an offence and shall be liable upon conviction to a fine or imprisonment for a term not exceeding five years, or both.

65. Computer related fraud

A person who, intentionally and without authorisation, causes loss of property to another person by;

(a) any input, alteration, deletion, delaying transmission or suppression of computer data; or;

(b) any interference with the functioning of a computer system, to procure on their behalf or on behalf of another person, any form of advantage, commits an offence and shall be liable upon conviction to a fine three times the value of undue

55. Offenses Related to Electronic Messages

A person who:

(a) unlawfully induces any person in charge of electronic devices to deliver any electronic messages not specifically meant for him or her;
(b) unlawfully hides or detains any electronic mail, message, electronic payment, credit and debit card which was found by the person or delivered to the person in error and which ought to be delivered to another person;
(c) unlawfully destroys or aborts any electronic mail or processes through which money or information is being conveyed;
(d) transfers, publishes, or disseminates, including making a digital depiction available for distribution or downloading through a telecommunications network or through any other means of transferring data to a computer, the intimate or obscene image of another person;
(e) knowingly and without authority causes any loss of property to another by altering, erasing, inputting or suppressing any data stored in a computer;
(f) sends an electronic message which materially misrepresents any fact upon which reliance by another person is caused to suffer any damage or loss;
(g) with intent to defraud, franks electronic messages, instructions, subscribes any electronic messages or instructions; or
(h) manipulates a computer or other electronic payment device with the intent to short pay or overpay.

commits an offence and upon conviction shall be liable to fine or imprisonment for a term not exceeding three years, or both.

Offences that Threaten National Security and Other Serious Crimes

56. Cyberterrorism

A person who intentionally accesses or causes to be accessed a computer system or network for the purpose of carrying out an act of terrorism, commits an offence and shall be liable upon conviction to a fine or imprisonment for a term not exceeding twenty years, or both.

57. Cyber Extortion

A person who engages in cyber extortion commits an offence and shall be liable upon conviction to a fine or imprisonment for a term not exceeding ten years, or both.

58. Human Trafficking

A person who establishes, publishes or shares information using a computer or computer system for the purposes of trafficking human beings or facilitating such a transaction commits an offence and upon conviction shall be liable to a fine or imprisonment for a term not exceeding seven years, or both.

59. Drug Trafficking

A person who creates, publishes or shares information using a computer or computer system for the purposes of trafficking in or distributing drugs or narcotics or facilitating such transaction commits an

(ii) in the case of paragraph (d) of this subsection, to a fine or imprisonment for a term not exceeding ten years or both.

(2) A person who, intentionally proposes, grooms or solicits, through any computer system or network, to meet a child for the purpose of engaging in sexual activities with the child by;
(a) use of coercion, inducement, force or threats;
(b) abuse of a recognized position of trust, authority or influence over the child, including within the family;
(c) abuse is made of a particularly vulnerable situation of the child, mental or physical disability or a situation of dependence; or
(d) recruiting, inducing, coercing, exposing, or causing a child to participate in pornographic performances or profiting from or otherwise exploiting a child for such purposes;

commits an offence under this Act and shall be liable upon conviction to a fine or imprisonment for a term not exceeding fifteen years, or both.

(3) For the purpose of subsection (1) of this section, the term "child pornography" includes 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; and
(c) realistic images representing a minor engaged in sexually explicit conduct.

51. Offensive Communication

A person who intentionally uses electronic devices to pass communication that is deemed harmful, abusive, or inappropriate, potentially causing harm or distress to others, commits an offence and upon conviction shall be liable to a fine or imprisonment for a term not exceeding two years, or both.

52. Cyberstalking

A person who intentionally and repeatedly uses electronic communication to track or monitor with intent to harass or cause fear to another person commits an offence and upon conviction shall be liable to a fine or imprisonment for a term not exceeding four years, or both.

53. Cyberbullying

A person who, individually or with other persons, commits cyberbullying, commits an offence and shall be liable upon conviction to a fine or imprisonment for a term not exceeding ten years, or both.

54. Cybersquatting

A person who intentionally takes or makes use of a name, business name, trademark, domain name or other word or phrase registered, owned or in use by another person on the internet or any other computer network without consent commits an offence and upon conviction shall be liable to a fine or imprisonment for a term not exceeding three years, or both.

45. Incitement Through Computer Systems

A person who incites another person or group of persons based on race, color, descent, nationality, gender, ethnic origin or religion through a computer system to commit violence or discrimination against another person or group of persons commits an offence and upon conviction shall be sentenced to imprisonment for a term not exceeding ten years or a fine, or both.

46. Spamming

(1) A person who, intentionally and without the consent of recipients, initiates the transmission of large-scale or repeated electronic messages through a computer system with intent to;
   (a) deceive or defraud any person; or
   (b) cause interference, disruption, or loss to any computer system or network commits an offence.
(2) Commercial or promotional messages sent with a valid opt-out mechanism shall not constitute an offence.
(3) A person convicted under this section shall be liable to a fine or imprisonment for a term not exceeding three years, or both

47. Phishing

A person who knowingly or intentionally;
(a) initiates the transmission of unsolicited messages;
(b) relays or retransmit unsolicited messages; or
(c) falsifies header information in unsolicited messages;

Commits an offence and shall be liable upon conviction to a fine or imprisonment for a term not exceeding five years, or both.

48. Pornography

A person who publishes or causes to publish pornographic photos, videos, books, magazines, films and other media through a computer system or any other information and communication technologies commits an offence and shall be liable upon-conviction to a fine or imprisonment for a term not exceeding ten years, or both.

49. Revenge Pornography

A person who, by means of a computer system, discloses or publishes a sexual photograph or film without the concept of the person who appears in the photographs or film, and with the intent of causing that person distress, commits an offence and shall be liable to a fine or imprisonment for a term not exceeding ten years, or both.

50. Child pornography and related offences

(1) A person who intentionally uses any computer system or network in or for;
   (a) producing child pornography.
   (b) distributing or transmitting child pornography.
   (c) procuring child pornography for oneself or for another person.
   (d) possessing child pornography in a computer system or on a computer-data storage medium:

commits an offence under this Act is liable upon conviction;

   (i) in the case of paragraphs (a), (b) and (c) of this subsection to a fine or imprisonment for a term not exceeding fifteen years or both; and

purpose, through a computer system;

(b) downloads movies, music files or pirated software applications for gain or against remuneration; or

(c) posts a copyrighted work such as writing or graphics, online for gain or remuneration, commits an offence.

(2) A person convicted under subsection (1) of this section, on;

(a) a first conviction shall be liable to a fine or imprisonment for a term not exceeding two years; and

(b) on a second or subsequent conviction, shall be liable to a fine or imprisonment for a term not exceeding seven years, or both.

42. Failure to moderate undesirable content

(1) An administrator of an online account or platform upon receipt of a written notice or order from an authorised investigating or regulatory authority, takes reasonable steps to restrict or remove access to unlawful content specified in the notice within a prescribed period.

(2) An administrator who fails to comply with subsection (1) of this section, commits an offence and shall be liable upon conviction to a fine or imprisonment for a term not exceeding five years, or both.

(3) For the purpose of this section "undesirable content" includes any online content that;

(a) is deceptive or inaccurate, posted with intent to defame, threaten, abuse or mislead the public;

(b) threatens public health or public safety;

(c) threatens national security; or

(d) promotes racism;

(e) Promotes Tribalism;

(f) Gender discrimination or bias.

43. Distribution of obscene or intimate images

A person who intentionally, through a telecommunications network or any other means of transferring data to a computer, transfers, publishes, disseminates, makes available for distribution, intentionally downloading a digital depiction that is intimate or obscene, images or sound recording or video of another person without that person's consent, commits an offence and shall be liable upon conviction to a fine or imprisonment for a term not exceeding ten years, or both.

44. Publication of False Information

A person who, through a computer system or network, intentionally publishes, disseminates or makes available information that the person knows to be false or misleading, with the intent that the information be acted upon or regarded as authentic, and the publication results in or is likely to result in any of the following;

(a) public panic, violence or serious public disorder;

(b) economic loss;

(c) damage to the reputation of any person or group of persons, commits an offence and shall be liable upon conviction to a fine or imprisonment for a term not exceeding five years or both.

39. Unauthorised interference

(1) A person who, intentionally and without authorisation, hinders the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer commits an offence and shall be liable upon conviction to a fine or imprisonment for a term not exceeding ten years, or both.
(2) For the purpose of this section, an interference is unauthorised if the person whose act causes the interference is not permitted to cause that interference.
(3) A person who commits an offence under subsection (1) of this section which:
  (a) results in financial loss to any person or organisation;
  (b) threatens national security;
  (c) causes reputational damage to any person;
  (d) causes physical or mental injury to, or the death of, any person;
  (e) causes, directly or indirectly, degradation, failure, interruption or obstruction of the operation of a computer system; or
  (f) threatens public health or public safety, is liable on conviction, to a fine not exceeding seventy-five million South Sudan pounds or to a term of imprisonment not exceeding ten years, or both;
(4) For the purpose of this section, it is immaterial whether or not the unauthorised interference is directed at;
  (a) any particular computer system, program or data;
  (b) a program or data of any kind; or
  (c) a program or data held in any computer system.
(5) For the purpose of this section, it is immaterial that an unauthorised interference or any intended effect of it is permanent or temporary.

40. Unauthorised modification of computer data

(1) Any person who, intentionally and without authorisation, modifies computer data commits an offence and shall be liable upon conviction to a fine or of imprisonment for a term not exceeding eight years, or both.
(2) Where, as a result of the commission of an offence under this section;
  (a) the operation of the computer system;
  (b) access to any computer program or computer data held in any computer; or
  (c) the operation of any computer program or the reliability of any such computer data, is suppressed, modified or otherwise impaired, a person who is convicted of the offence shall be liable to a fine or imprisonment for a term not exceeding eight years or both;
(3) A modification is unauthorised if the person whose act causes the modifications, is not permitted to cause such modifications.
(4) For the purpose of this section, it is immaterial whether an unauthorised modification, or any intended effect of it, is permanent or temporary.

41. Infringement of copyright and related rights

(1) A person who, without the express authorisation of the author or owner of the copyright;
  (a) attempts to use, publish or distribute another person's work for commercial

such right in good faith;

(b) has expressed or implied consent of the person empowered to authorise him to have such an access;

(c) has reasonable grounds to believe that the person had such consent as specified in paragraph (b) of this section;

(d) is acting pursuant to measures that can be taken under this Act; or

(e) is acting in reliance of any statutory power arising under any enactment for the purpose of obtaining information, or of taking possession of any document or other property.

36. Unauthorised disclosure of password

A person who, intentionally and without authorisation, discloses any password, access code, biometric authentication, token, two-factor authentication, multi-factor authentication or any other means of gaining access to any computer program or computer data held in any computer system for its production, sale, procurement for use, import or distribution commits an offence and shall be liable upon conviction to a fine or imprisonment for a term not exceeding five years, or both.

37. Identity theft and impersonation

A person who:

(a) intentionally uses somebody's identity over the internet in bad faith to profit, mislead or destroy reputation, if such identity is similar, undistinguishable, or confusingly similar to an existing name or description that belongs to another person or organ;

(b) knowingly or wilfully, while not being a manufacturer of a computer system or an authorized agent of the manufacturer, changes computer system equipment identity or the process of accessing to it;

(c) fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person commits an offence and shall be liable to a fine or imprisonment for a term not exceeding fifteen years, or both.

38. Unauthorised interception of computer service

(1) A person who, by any technical means, wilfully intercepts or causes to be intercepted without authorisation, any computer data, or electromagnetic emissions carrying computer data, or non-public transmissions to, from or within a computer system commits an offence and shall be liable upon conviction to a fine or imprisonment for a term not exceeding seven years, or both.

(2) Where, as a result of the commission of an offence under subsection (1) of this of this section, the operation of the computer system is impaired, or transmitted computer data is suppressed or modified, a person convicted of that offence shall be liable to a fine or imprisonment for a term not exceeding three years, or both.

(3) For the purpose of this section, it is immaterial that the unauthorised interception is not directed at;

(a) any particular program or data;

(b) a program or data of any kind; or

(c) is acting in the performance of his lawful duties, contractual obligations or is discharging any legal obligation.

CHAPTER VI
OFFENCES AND PENALTIES

33. Unauthorized Data Transmission

(1) A person who, intentionally and without lawful authority or consent;
   (a) communicates, discloses, transmits, or makes available any computer data, information system program, access code, or command to another person knowing that such transmission is unauthorized; or
   (b) intentionally and unlawfully receives or uses computer data obtained in the manner described in paragraph (a), commits an offence.

(2) A person convicted under subsection (1)(a) of this section shall be liable upon conviction to a fine or imprisonment for a term not exceeding five years or both.

34. Unlawful possession of devices and computer data

(1) A person who:
   (a) intentionally manufactures, sells, procures for use, imports, distributes or otherwise makes available, a computer system, computer data or any other device, designed or adapted primarily for the purpose of committing any offence under this Act commits an offence.
   (b) intentionally and without authorisation, receives or is in possession of devices and computer data under subsection of this section (a) commits an offence.
   (c) a person who commits an offence under this section shall be liable upon conviction to a fine or imprisonment for a term not exceeding ten years, or both.

(2) In this section, possession of any computer data includes;
   (a) having possession of a computer system or device that holds or contains the computer data or computer program.
   (b) having possession of a document in which the computer data or computer program is recorded; or
   (c) having control of computer data or computer program that is in the possession of another person.

35. Unauthorised access to computer data

(1) Any person who gains unauthorised access to any program or data held in a computer system commits an offence and shall be liable upon conviction to a fine or imprisonment for a term not exceeding three years, or both;

(2) Access by a person to a computer system is unauthorised where the person is not entitled to control access of the kind in question and not authorized to access.

(3) For the purpose of this section, it is immaterial that the unauthorised access is not directed at;

   (a) any particular program or data;
   (b) a program or data of any kind; or
   (c) a program or data held in any particular computer system.

(4) A person is not liable under subsection (1) of this section if that person;
   (a) has a right to control the operation or use of the computer system and exercises

(2) A person who contravenes subsection (1) of this section commits an offence and shall be liable upon conviction to a fine or a term of imprisonment not exceeding five years, or both.

(3) Where the offence committed under subsection (1) of this section;

(a) results in a serious bodily injury, financial loss or damage to the computer system or computer network designated as a critical information infrastructure, the person who committed the offence;

(i) in the case of an individual, shall be liable upon conviction to a fine or a term of imprisonment not exceeding fifteen years or both;

(ii) in the case of a body corporate, a partnership or a firm shall be liable upon conviction to a fine.

(b) is deemed to be a terrorist act, the person who committed the offence shall be liable upon conviction to a term of imprisonment of not exceeding twenty-five years.

(4) Where an offence under subsection (3) of this section is committed by a body corporate or by a member of a partnership or other firm, every director or officer of that body corporate or a member of the partnership or any other person concerned with the management of the firm is deemed to have committed that offence shall be liable upon conviction to a fine;

(5) A person shall not be convicted of an offence by virtue of subsection (4) of this section if it is proved that;

(a) due diligence was exercised to prevent the commission of the offence; and

(b) the offence was committed without the knowledge, consent or connivance of that person.

32. Responsibility of the Authority Relating to Response to Cybersecurity Incident

(1) The Authority shall establish a national computer incident response team coordination centre (SS-CIRT/CC) to serve as a point of contact to identify, defend, respond and resolve cybersecurity incidents.

(2) The cybersecurity coordination centre (SS-CIRT/CC) shall serve as the focal point for all instances of cybersecurity incidents by:

(a) providing technical analysis of computer security incidents,

(b) conducting awareness campaigns and training programs, empowering individuals, and organizations with the knowledge to protect themselves against cyber threats,

(c) issuing relevant alerts and advisories on emerging threats to computer security thus helping individuals and organizations enhance their cybersecurity posture,

(d) providing timely, actionable insights into emerging threats and vulnerabilities,

(e) coordinating cyber security incident responses with trusted third parties.

(3) The cybersecurity coordination centre shall establish a cyber security incident reporting and information sharing platform to enable public to report a cybersecurity incident.

27. Registration of critical infrastructure

(1) The Authority shall register a critical infrastructure.
(2) The Authority shall, by publication, determine;
  (a) the requirements for the registration of a critical infrastructure.
  (b) the procedure for the registration of a critical infrastructure; and
  (c) any other matter relating to the registration of a critical infrastructure.

(3) Where there is any change in the legal ownership of a registered critical infrastructure, the owner of the registered critical infrastructure shall, within seven days after the change, inform the Authority of the change in ownership.
(4) An owner of a registered critical infrastructure who contravenes subsection (3) of this section is liable to pay to the Authority the administrative penalty prescribed by the minister.

28. Withdrawal of designation of critical infrastructure

The Competent Minister may, on the advice of the Authority and by publication in the *Gazette*, withdraw the designation of a critical infrastructure at any time if the minister considers that the computer system or computer network no longer satisfies the criteria of a critical infrastructure.

29. Management and compliance audit of critical infrastructure

(1) The Competent Minister shall prescribe minimum standards for prohibitions in respect of the general management of a critical infrastructure that the minister considers necessary for the protection of national security.
(2) The Authority shall carry out a periodic audit and inspection on a critical infrastructure to ensure compliance with the provisions of this Act.

30. Duty of owner of critical infrastructure

(1) An owner of a critical infrastructure shall;
  (a) report a cybersecurity incident within twenty-four hours after the incident is detected to the Authority.
  (b) cause an audit to be performed on a critical infrastructure; and
  (c) submit a copy of the audit report to the Authority.

(2) An owner of a critical infrastructure who contravenes the provisions of sub section (1) of this section, is liable to pay to the Authority the administrative penalty that may be prescribed by the minister.

31. Access to critical infrastructure

(1) A person shall not without authorisation;
  (a) secure access, or
  (b) attempt to secure access to a computer system or a computer network designated as a critical infrastructure.

(a) accordance with any other law,
(b) compliance with an order from a Court,
(c) relation to the prevention of injury or other damage to the health of a person or serious loss of, or damage to property; and
(d) the public interest.

(2) Subject to subsection (1) of this section any person authorised by the investigatory Unit shall, on receipt of a request, in writing permit a person who had the custody or control of a computer system to access and copy computer data on the computer system.

(3) A person authorised, in writing, by the investigatory Unit, may refuse to give access to computer data or provide copies of such computer data if he has reasonable grounds to believe that;
(a) possession of the data constitutes, or may lead to, or assist in, a criminal offence; or
(b) in connection with which the search was carried out, another ongoing investigation, or any criminal proceedings that are pending or which may be brought in relation to any of those investigations.

CHAPTER V
CRITICAL NATIONAL INFRASTRUCTURE

26. Designation of critical infrastructure.

(1) The competent minister may, on the advice of the Authority, designate a computer system or computer network as a critical infrastructure if the minister considers that the computer system or computer network is essential for;
(a) national security, or
(b) the economic and social well-being of citizens.

(2) Where the minister designates a computer system or computer network as a critical infrastructure, the minister shall publish the designation in the *Gazette*.

(3) The minister shall, in making a determination under subsection (1) of this section, consider if the computer system or computer network is necessary for;
(a) the security, defence or international relations of the country,
(b) the production, preservation of the identity of a confidential source of information related to the enforcement of cybercrime and other related criminal law,
(c) the provision of services directly related to;
(i) communications and telecommunications infrastructure,
(ii) banking and financial services,
(iii) public utilities,
(iv) public transportation; and
(v) public key infrastructure.
(d) the protection of public safety and public health, including systems related to essential emergency services.
(e) an international business or communication affecting a citizen of the Republic of South Sudan or any other international business in which a citizen of the Republic of South Sudan or the Government has an interest; or
(f) the Legislature, Executive, Judiciary, Public Services or security agencies.

(4) The minister shall, by publication in the *Gazette*, establish the procedure for the regulation of a critical infrastructure.

(c) maintain the integrity of the relevant stored computer data,
(d) conduct forensic analysis or examination of the computer data storage medium,
(e) render inaccessible or remove those computer data from the accessed computer system.

(3) The investigatory Unit may 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 reasonable, the necessary information, to enable the undertaking of the measures referred to in subsections (1) and (2) of this section.

22. Real-time collection of traffic data

Where the investigatory Unit has reasonable grounds to believe that traffic data is relevant for the purpose of investigation and prosecution of an offence, it may make an application to the Judge in Chambers for an order:

(a) authorising the collection or recording of traffic data on the Republic of South Sudan territory by technical means, in real-time, associated with specified communications transmitted by means of any computer system.
(b) compelling a service provider, within its technical capabilities, to;
  (i) effect such collection and recording specified in paragraph (a) of this section; or
  (ii) cooperate with the investigatory Unit to effect such collection and recording;
(c) compelling a service provider to keep confidential the fact of the execution of any power provided under this section and any information relating to it.

23. Interception of Content Data

Where the investigatory Unit has reasonable grounds to believe that any content data is relevant for the investigation and prosecution of an offence, it may make an application to the court for an order to;

(a) collect or record content data in the territory of the Republic of South Sudan by technical means in real-time of specified communications by means of a computer system.
(b) compel a service provider, within its existing technical capabilities, to;
  (i) collect or record by technical means in the Republic of South Sudan.
  (ii) cooperate and assist the investigatory Unit in the collection or recording of content data in real-time of specified communications in the Republic of South Sudan, transmitted by means of a computer system; or
(c) compel a service provider to keep the confidentiality of the fact of the execution of any power provided for in this section and any information relating to it.

24. Deletion Order.

The Court may, for the purpose of this Act, upon application by the investigatory Unit, and upon being satisfied that a computer system or any other device contains any unlawful material or activity, order that such computer data be;

(a) no longer stored on and made available through the computer system or any other device; or
(b) deleted or destroyed.

25. Limited use of disclosed computer data and information.

(1) Computer data obtained under this Act by any person authorised, in writing, by the investigatory Unit shall be used for the purpose of a criminal investigation or the prosecution of an offence, unless such computer data is sought in;

(2) preserve data and evidence;
(3) obtain information and detect suspects;
(4) issue and promulgate guidelines, advisories, and procedures in all matters related to cybercrime investigation, forensic evidence recovery, and forensic data analysis consistent with industry standard practices; and
(5) prescribe forms and templates, including, but not limited to, those for preservation orders, chain of custody, consent to search, consent access to an account or online identity, and request for computer forensic examination.

19. Expedited preservation and partial disclosure of traffic data

(1) Where the investigatory Unit has reasonable grounds to believe that;
(a) any specified traffic data stored in any computer system or device, or by means of a computer system, is reasonably required for the purpose of a criminal investigation; and
(b) there is a risk that the traffic data may be modified, lost, destroyed or rendered inaccessible. The investigatory Unit shall serve a notice on the person who is in possession or control of the traffic data, requiring the person to;
(i) undertake expeditious preservation of such available traffic data regardless of whether one or more service providers were involved in the transmission of that communication; or

(ii) disclose required traffic data concerning that communication in order to identify the service providers and the path through which communication was transmitted.

(2) The data specified in the notice referred to in subsection (1) of this section shall be preserved and its integrity shall be maintained for a period not exceeding 90 days.

20. Production Order

(1) Where the disclosure of data is required for the purpose of a criminal investigation or prosecution of an offence, the investigatory Unit may make an application to the Court for an order compelling;
(a) a person in the Republic of South Sudan to submit specified data in that person's possession or control, which is stored in a computer system or device.
(b) any service provider offering its services in the Republic of South Sudan to submit subscriber information in relation to such services in that service provider's possession or control.

(2) Where any material, to which an investigation relates, consists of computer data stored in a computer system, the request shall be deemed to require the person to produce or give access to it in a form in which it can be taken away and in which it is easily understood.

21. Powers of access, search and seizure for purpose of investigation

(1) Where the investigatory Unit has reasonable grounds to believe that;

(a) stored data is relevant for the purpose of an investigation or the prosecution of an offence, it may make an application to court for the issue of a warrant to enter any premises to access, search and seize such data,
(b) data sought is stored in another computer system or part of it in the Republic of South Sudan territory, and such data is lawfully accessible from or available to the initial system, the investigatory Unit shall expeditiously extend the search or similar access to the other systems.

(2) The investigatory Unit may, in the execution of a warrant under subsection (1),
(a) seize or secure a computer system or part of it or a computer data storage medium,
(b) make and retain a copy of those computer data,

(3) The Authority shall, on receipt of the request under this section, take all appropriate measures to obtain necessary authorisation, including any warrant to execute upon the request in accordance with the procedures and powers provided under this Act and any other relevant law.
(4) Where the Authority obtains the necessary authorisation, including any warrant to execute upon the request, the Authority may seek the support and cooperation of the requesting State during the collection.
(5) The Authority shall, upon conducting the measures under this section, and subject to section 22 provide the results to the requesting State.

16. Mutual assistance regarding interception of content data

(1) A requesting State may request the Authority to provide assistance in the real-time collection or recording of content data of specified communications in South Sudan transmitted by means of a computer system.
(2) When making a request under subsection (1) of this section, a requesting State shall specify;
(a) the authority seeking the use of powers under this section.
(b) the offence that is the subject of a criminal investigation or proceedings and a summary of the related facts.
(c) the name of the authority with access to the relevant communication.
(d) the intended duration of the interception.
(e) the reason for using powers under this section; and
(f) the terms and conditions of the use and disclosure of the communication to third parties.
(3) The Authority shall, on receipt of the request under this section, take appropriate measures as may be required to obtain necessary authorisation, including any warrant to execute the request in accordance with this Act and any other relevant legislation.
(4) Where the Authority obtains the necessary authorisation, including any warrant to execute upon the request, the Unit may seek the support and cooperation of the requesting State during the interception.
(5) The Authority shall, upon conducting the measures under this section, provide the results to the requesting State.

CHAPTER IV
ESTABLISHMENT OF CYBERCRIME PROSECUTION UNIT

17. The National Cybercrime Prosecution Unit

(1) There shall be established a Cybercrime Prosecution Unit (hereafter referred to as the Unit).
(2) The Unit shall be under the Ministry of Justice and Constitutional Affairs.
(3) The Minister shall by regulation, prescribe the composition, qualifications and staff requirements of the Unit.

18. Powers and functions of the Unit

The Unit shall be competent to:
(1) investigate and prosecute cybercrimes and other violations under this Act;

(l) give any other information that may assist in giving effect to the request.

(3) The Authority shall, on receiving the request under this section, take such appropriate measures as may be required to obtain necessary authorisation, including any warrants, to execute the request in accordance with this Act and any other relevant law.

(4) Where the Authority obtains the necessary authorisation in accordance with subsection (3) of this section, including any warrants, to execute the request, the Authority may seek the support and cooperation of the requesting State during such search and seizure.

(5) For the purpose of conducting the search and seizure request, the Authority shall provide to the requesting State, the results of the search and details in respect of any electronic or physical evidence seized.

(6) The request shall be responded to on an expedited basis where;
(a) there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or
(b) any relevant laws so required.

14. Trans border access to stored computer data with consent or where publicly available

The investigatory unit may, without the authorisation of another State, and subject to this Act;

(a) access publicly available stored computer data, regardless of where the data is located geographically; or
(b) access or receive, through a computer system in the Republic of South Sudan, stored computer data located in another State, if a police officer or authorised person obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Republic of South Sudan through that computer system.

15. Mutual assistance in real-time collection of traffic data

(I) A requesting State may request the Authority to provide assistance in real-time collection of traffic data associated with specified communications in the Republic of South Sudan, transmitted by means of a computer system.

(2) For the purpose of subsection (1) of this section, the requesting State shall specify;

(a) the authority seeking the use of powers under this section.
(b) the offence that is the subject of a criminal investigation or proceedings and a summary of the related facts.
(c) the name of the authority which has access to the relevant traffic data.
(d) the location at which the traffic data may be held.
(e) the intended purpose of requiring the traffic data.
(f) such information as may be required to identify the traffic data.
(g) any further details relevant to the traffic data.
(h) the reason for using powers under this section; and
(i) the terms and conditions for the use and disclosure of the traffic data to third parties.

(4) The data shall, on receipt for a request under this section, continue to be preserved pending the final decision being made with regards to that request.

12. Expedited disclosure of preserved traffic data

(1) Where, in the course of executing a request under section 19 with respect to a specified communication, the investigating agency discovers that a service provider in another State was involved in the transmission of the communication, the Authority shall expeditiously disclose to the requesting State a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.

(2) Disclosure of traffic data under paragraph (a) of this section may only be withheld if the Authority considers that the execution of the request is likely to prejudice the Republic of South Sudan's sovereignty, security, public order or public interest.

13. Mutual assistance regarding accessing of stored computer data

(1) A requesting State may request the Inspector General of Police, through the Authority, to search or similarly access, seize or similarly secure, and disclose stored computer data located within the Republic of South Sudan, including computer data that are specified in section 19 of this Act..

(2) For the purpose of subsection (1) of this section, the requesting State shall;

(a) provide the name of the authority conducting the investigation or proceedings to which the request relates;
(b) give a description of the nature of the criminal matter and a statement setting out a summary of the relevant facts and laws;
(c) give a description of the purpose of the request and the nature of the assistance being sought;
(d) in the case of a request to restrain or confiscate assets believed, on reasonable grounds, to be located in the Republic of South Sudan, give details of the offence, particulars of the investigation or proceedings commenced in respect of the offence, and be accompanied by a copy of any relevant restraining or confiscation order;
(e) give details of any procedure that the requesting State wishes to be followed by the Republic of South Sudan in giving effect to the request, particularly in the case of a request to take evidence;
(f) include a statement setting out any demands of the requesting State concerning any confidentiality relating to the request and the reasons for those demands;
(g) give details of the period within which the requesting State wishes the request to be complied with.
(h) where applicable, give details of the property, computer system or device to be traced, restrained, seized or confiscated, and of the grounds for believing that the property is believed to be in the Republic of South Sudan.
(i) give details of the stored computer data or program to be seized and its relationship to the offence.
(j) give any available information that may identify the custodian of the stored computer data or the location of the computer system or device.
(k) include an agreement on the question of the payment of the damages or costs of fulfilling the request; and

10. Spontaneous Information

(1) The Authority may, subject to this Act and any other relevant law, without a prior request, forward to a foreign State information obtained within the framework of a South Sudan investigation where it considers that the disclosure of such information may;

(a) assist the foreign State in initiating or carrying out investigations or proceedings concerning criminal offences related to cybercrime and computer misuse; or

(b) lead to a request for cooperation by the foreign State under this Act.

(2) Prior to providing the information under subsection (1) of this section, the Authority may request that such information be kept confidential or disclosed only subject to such conditions as may be specified.

(3) Where a foreign State does not comply with the conditions specified under subsection (2) of this section, the State shall forthwith notify the Authority.

(4) The Authority shall, on receipt of a notice under subsection (3) of this section, determine whether the foreign State should be provided the information requested for.

(5) The Authority may refuse to provide the information where the foreign State does not take the commitment to respect the conditions specified by the Unit.

11. Expedited preservation of stored computer data

(1) A requesting State which intends to make a request for mutual legal assistance for the search or similar access, seizure or similar securing or the disclosure of computer data, may request the Authority to obtain the expeditious preservation of stored computer data located within the territory of South Sudan.

(2) The requesting State shall, in its request under subsection (1) of this section, specify;

(a) the name of the authority seeking the preservation.

(b) the offence that is the subject of a criminal investigation or proceedings and a summary of the related facts.

(c) the stored computer data to be preserved and its connection to the offence.

(d) any available information identifying the custodian of the stored computer data or the location of the computer system.

(e) the necessity of the preservation; and

(f) the intention to submit a request for mutual assistance for the search or similar access, seizure or similar securing or the disclosure of the stored computer data.

(3) The Authority shall;

(a) on receipt of the request under this section, take appropriate measures to preserve the specified data in accordance with the procedures set out in, and powers conferred under this Act and any other relevant legislation.

(b) The purpose of the preservation of stored computer data effected under this section shall be to enable the State to submit a request for the search or access, seizure or securing, or the disclosure of the data.

(c) The stored computer data shall be preserved for a period not exceeding 180 days.

CHAPTER III
INTERNATIONAL COOPERATION

8. International Cooperation

(1) The Authority shall in the performance of its functions, promote the security of cyberspace through international co-operation.

(2) The Authority shall implement relevant measures for the effective implementation and enforcement of international treaties on cybercrime, of which South Sudan is a signatory.

9. General Principles Relating to International Cooperation

(1) The Authority may make a request for mutual legal assistance in any criminal matter to a foreign State for the purpose of;

(a) undertaking investigations or proceedings concerning offences related to computer systems, electronic communications or computer data,

(b) collecting evidence of an offence in electronic form,

(c) collecting evidence in electronic form of any criminal offence not limited to offences under this Act; or

(d) obtaining expeditious preservation and disclosure of data, including traffic data, real-time collection of traffic data associated with specified communications or interception of computer data or any other means, power, function or provisions under this Act.

(2) For any of the purposes listed in subsection (1)(a) to (d) of this section, a requesting State may make a request for mutual legal assistance to the Authority in any criminal matter.

(3) Where a request is received under subsection (2) of this section, the Authority may, subject to this Act and any other relevant law grant the legal assistance requested.

(4) The Authority may require a requesting State to;

(a) keep the contents, information and materials provided in a confidential manner;

(b) only use the contents, information and materials provided for the purpose of the criminal matter specified in the request; and

(c) use the contents, information and materials subject to such conditions as may be specified.

(5) Prior to providing any information, the Authority may request that it be kept confidential or only used subject to such conditions as may be specified.

(6) If the receiving Party cannot comply with such a request, it shall notify the Authority accordingly, which shall then determine whether the information should nevertheless be provided.

(7) Where, subject to subsections (5) and (6) of this section, a receiving party accepts the information, it shall comply with the conditions specified.

CHAPTER II
OBLIGATIONS OF SERVICE PROVIDERS AND JURISDICTION OF CYBERCRIMES AND COMPUTER MISUSE ACT

6. Obligations of Service Providers

(1) Without prejudice to the National Communication Act, 2012 a service provider shall:
   (a) Keep, store, record information system or any means of information technologies for continuous period of 180 days, data to be saved include the following:
      (i) Data that enables the identification of the user of the data service related to the information system in which he deals with whenever the service provider is in control.
      (ii) Traffic data.
      (iii) data on peripheral devices for any communication.
      (iv) any other data specified by the National Communication Authority.
   (b) Take reasonable steps to inform its clients of cybercrimes trends which affect or may affect its clients.
   (c) Disclose abuses to the concerned victim and to relevant authorities that infractions are committed.
   (d) Maintain confidentiality of the data saved and stored and not disclosing them without an order from competent judicial authority, this includes:
      (i) Personal data of any user of these services or any data or information related to the consent and the provided account that this users or person entered communication with.
      (ii) Securing data and information in a way that preserves its biography and not penetrating or damaging it.

(2) Without prejudice to the privacy guaranteed by the Constitution, service providers and its agents are obliged to comply with relevant law enforcement agencies in accordance with technical capabilities in allowing operation of the law.

(3) Without prejudice to the provisions of Consumer Protection Act, 2011 the service providers shall provide its users and specialised government agencies, in the form and method that can be easily accessed directly and continuously, the following data and information:
   (a) The name, address, electronic address, information data of service provider.
   (b) Any other information that the National Communication Authority considers important for the protection of users.

7. Jurisdiction of Cybercrimes and Computer Misuse

Without prejudice to the provisions of the Penal Code, 2008, the provisions of this Act shall apply to a crime committed in or outside the country, which shall occur in the following cases:

(a) By any means of transportation including vehicle, aircraft or ship registered in the Republic of South Sudan.
(b) By a South Sudanese.
(c) If a victim is a South Sudanese.
(d) If the preparation, planning, direction, supervision and funding in the Republic of South Sudan.
(e) If the crime committed by an organised terrorist group that carries out criminal activities in more than one country including the Republic of South Sudan.
(f) By any person, irrespective of his or her nationality, citizenship or location.
(g) If the perpetrator of the crime is found in the Republic of South Sudan after its commission and has not been extradited.

"Real-time" means the way a computer system receives data and then communicates it or makes it available immediately;

"Service" means use of image, audio, video or data provided over internet or other electronic means.

"Service Provider" means:

(a) a public or private entity that provides to users of its services the means to communicate by use of a computer system, and

(b) any other entity that processes or stores computer data on behalf of that entity or its users;

"Spamming" means using messaging systems to send multiple unsolicited messages to a large number of recipients for the purpose of commercial advertising, non-commercial proselytising, or any prohibited purpose;

"SS-CIRT" means the South Sudan Computer Incident Response Team established pursuant to section 32(1) of this Act;

"Subscriber Information" means any information contained in the form of data or any form that is held by a service provider, relating to subscribers of its services, other than traffic data or content data, by which can be established by,

(a) the type of communication service used, the technical provisions taken thereto and the period of service,

(b) the subscriber's identity, postal, geographic location, electronic mail address, telephone and other access number, Acting and payment information, available based on the service agreement or arrangement; or

(c) any other information on the site of the installation of telecommunication apparatus, available on the basis of the service agreement or arrangement.

"Traffic data" means any computer data other than the content of the communication, including, but not limited to the communication's origin, destination, route, time, date, size, duration, or type of underlying service;

"Unauthorised access" means access of any kind by a person to a programme or data held in a computer without permission if;

(a) The person is not personally entitled to control access of the kind in question to the programme or data; and

(b) The person does not have consent to access the kind of programme or data from the person who is entitled to control access;

"Webpage" means any sources of information stored electronically which may be accessed through hyperlinks or any information network;

"Website" means a group of World Wide Web pages usually containing hyperlinks to each other and made available online by an individual, company, educational institution, government or organisation.

"Information System" means a system for generating, sending, receiving, storing, displaying or otherwise processing data messages; and includes the internet or any other information sharing system;

"Integrity" means the accuracy, consistency, and reliability of data;

"Interception" means listening to, recording, monitoring or surveillance of the content of communication, including procuring of the content of data, either directly through access and use of computer, a computer system or indirectly, through the use of electronic eavesdropping or tapping devices, when communication is occurring;

"Interference" means any impairment to the confidentiality, integrity or availability of a computer system or any program or data on a computer system, or any act in relation to the computer system, which impairs the operation of the computer system, program, or data;

"Investigatory Unit" means the National Cybercrime Prosecution Unit established by section 17 of this Act;

"Means of Communication" means information and communication devices, including computers, or smart devices or similar related devices;

"Minister" means the Minister responsible for Justice and Constitutional Affairs.

"Mobile Money" means electronic transfer of funds between mobile phone network subscribers, banks or accounts deposits or withdrawals of funds or payment of Acts or processing financial transactions by mobile devices;

"National Critical Information Infrastructure: means a vital virtual asset, facility, system, network or process whose incapacity, destruction or modification would have;

(a) a debilitating impact on the availability, integrity or delivery of essential services including those services, whose integrity, if compromised, could result in significant loss of life or casualties; or

(b) significant impact on national security, national defence or the functioning of the state.

"Network" means a collection of hardware and computers interconnected by communications channels that allow sharing of resources and information;

"Owner of critical information infrastructure" means the legal owner or operator of the critical information infrastructure and, where the critical information infrastructure is jointly owned by more than one person, includes every joint owner.

"Password" means any data by which a computer service or a computer system is capable of being accessed for use;

"Pornography" includes the representation in books, magazines, photographs, films, and other media, telecommunication apparatus of scenes of sexual behaviour that are erotic or lewd and are designed to arouse sexual interest;

"Phishing" means the practice of sending fraudulent communications that appear to come from a legitimate source by email, text message or other forms of communication with the intention to steal money, gaining access to sensitive data and login information, or to install malware on the victim's device;

"Public key infrastructure" means a system of hardware, software, policies, and procedures used to create, manage, distribute, and revoke digital certificates that verify the ownership of public keys, allowing for secure online communication and authentication between entities;

"Publish" means distributing, transmitting, disseminating, circulating, delivering, exhibit, exchanging, barter, printing, copying, selling or offering in any other way or making available in any way;

"Reception" means acquisition of data or information contained in any malicious electronic message;

"Cyber Espionage" Means use of computer device or computer system to obtain secret or confidential information on critical infrastructure, security infrastructure and leadership;

"Cyber Extortion" cyber extortion is a form of cybercrime where a person threatens to damage, disable, or release a data system, or network, unless a ransom is paid or a demand is made often under the threat of harming or exposing sensitive digital assets;

"Data" means numbers, letters, symbols or electronic representations of information in any form stored, processed, generated, produced, transferred to a computer or other electronic device;

"Database" means electronic space in which data and information are organised and stored in a way which enable its retrieval or modification;

"Device" includes;

(a) a computer program, code, software or application,

(b) component of computer system such as graphic card, memory card, chip or processor,

(c) computer storage component,

(d) input and output devices.

"Digital Forensic Expert or Forensic Expert" means an expert with knowledge in the field of digital forensics by training, practice, experience, certification, formal education on digital forensics or other qualifications;

"Economic Sabotage" Means deliberate use of a computer device or computer system to harm or disrupt an economic interest of the country and individual.

"Electronic" means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities, and the word "electronically" shall be similarly construed;

"Electronic Communication" means any transfer of a sign, signal or computer data of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic, photo optical system in any other similar form physically or virtually;

"Forensics" means the application of investigative and analytical techniques that conform to evidentiary standards, and are used in, or appropriate for, a court of law or another legal context;

"forensic image" also known as a forensic copy, means an exact bit-by-bit copy of a data carrier, including slack, unallocated space and unused space;

"Forensic Tool" means any investigative tool or device including software or hardware installed on or in relation to a computer system or part of a computer system and used to perform tasks including keystroke logging or collection of investigation information about a use of a computer or computer system by an expert;

"Hosting Provider" means a person who provides service that run servers connected to internet allowing organisation and individual to serve content or host services connected to internet;

"Hyperlink" means a symbol, word, phrase, sentence or image that contains path to another source that points to and causes to display other documents when executed;

"Indecent Content" means any data, information, audio, image, data message, photo, document, video, graphical representation or symbol that is contrary to the norms and traditions;

"Information" means data, text, images, sounds, codes, computer programs, software and databases;

"Cybercrime" means any crime committed through information system, networks, software, computer, internet or any related activities;

"Cyber security" means the state in which a computer or computer system is protected from unauthorised access or attack for the purpose of ensuring that;

(a) the computer or computer system continues to be available and operational.

(b) the integrity of the computer or computer system is maintained; and

(c) the integrity and confidentiality of information stored in, processed by or transmitted through the computer or computer system is maintained.

"Cyber security Incident" means any act or attempt, successful or unsuccessful, to gain unauthorised access to, disrupt or misuse an information system or information stored on such information system.

"Cyber security Products" includes:

(a) a computer;

(b) a computer system;

(c) a computer programme; or

(d) a computer service designed for, or purported to be designed for, ensuring or enhancing the cybersecurity of another computer or computer system.

"Cyber Terrorism" means criminal acts committed by individual or group to further violence or ideological goals streaming from domestic influences, political, religious, social, racial or environmental nature or associated with, designed foreign terrorist organisation or states sponsor;

"Cyber Terrorist act" means an act performed in furtherance of a political, ideological, religious, racial or ethnic cause and

(a) causes serious bodily harm to a person.

(b) causes serious damage to property.

(c) endangers the life of a person.

(d) Creates a serious risk to the health or safety of the public.

(e) Involves the use of firearms or explosives.

(f) releases into the environment or exposes the public to:

(i) Dangerous, hazardous, radioactive or harmful substances.

(ii) Toxic chemicals; or

(iii) microbial or other biological agents or toxins.

(g) is prejudicial to national security or public safety.

(h) is designed or intended to disrupt—

(i) A computer system or the provision of services directly related to communications.

(j) Banking or financial services; or

(k) Utilities or transportation.

"Cyber security threat" means an unauthorised effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system;

"Ccyberspace" means the connected network of information technology infrastructure comprising telecom networks, the internet, computer networks, information systems, information processing and control systems and databases where people perform social acts without being limited by space and time;

"Cyber security Service Provider" means a person licensed to provide a cyber security service;

"Application" means programme or software used to provide electronic or digital services or execution of what the user may need through any means of information;

"Authority" means the National Communication Authority established under section 12 of the National Communication Act, 2012;

"Availability" means the ability to make information and related resources accessible as needed, when they are needed, where they are needed;

"Access" means instruction, communication with, storing data in, retrieving data from, or otherwise making use of any resources of computer system or communication networks;

"Communication" the transmission of information through physical or virtual information communication technologies media;

"Communication Network" means any connection between more than one system or communication;

"Communication Structure" means private information systems and other sensitive information for provision of service to the public;

"Competent Minister" means the Minister responsible for communication;

"Computer" means an electronic, magnetic, optical, electrochemical, or other data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device;

"Computer system" means an arrangement of interconnected computers that is designed to perform one or more specific functions, and includes

(a) an information system; and

(b) an operational technologies system, a programmable logic controller, a supervisory control and data acquisition system, or a distributed control system.

"Computer data" means 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 and includes electronic documents or electronic data messages whether stored in local computer systems or online;

"Computer program" means a set of instructions executed by the computer to achieve intended results;

"Content data" means the communication content of the communication, the meaning or purpose of the communication, or the message or information being conveyed by the communication, other than traffic data;

"Confidentiality" means the state of keeping or being kept secret or private;

"Critical Information Infrastructure" means systems, assets, programme or data that are so vital to the country that their destruction would have an impact on the security, national economic security, national public health and safety of the countr;

"Critical Infrastructure" means the processes, systems, facilities, technologies, networks, assets, and services essential to the health, safety, security or economic wellbeing of south Sudanese and the effective functioning of Government;

"Cyber bullying" Means a hurtful, targeted behavior using digital platforms such as, social media, texts, and an online game. It involves the repeated and intentional use of digital technologies to harass, threaten, embarrass, or target another person;

LAWS OF SOUTH SUDAN
CYBERCRIMES AND COMPUTER MISUSE ACT, 2026

In accordance with the provisions of Article 55 (2) and (3)(b) of the Transitional Constitution of the Republic of South Sudan, 2011 (as amended) the National Legislature, hereby enacts the following:

CHAPTER I
PRELIMINARY PROVISIONS

1. Title and Commencement

This Act shall be cited as "the Cybercrimes and Computer Misuse Act, 2026" and shall come into force on the date of its signature by the President.

2. Repeal and Saving

Any legislation governing the subject of this Act is hereby repealed; provided that, all actions taken, proceedings, appointments, orders and regulations made or issued thereunder shall remain in force until they are repealed or amended in accordance with the provisions of this Act.

3. Purpose

The Purpose of this Act is;

(a) To provide for offences relating to computer systems to enable timely and effective detection, prohibition, prevention, investigation and prosecution of computer and cybercrimes.

(b) To facilitate international cooperation in dealing with computer and cybercrimes matters, and for related purposes.

4. Authority and Application

(1) This Act is drafted in accordance with the provisions of Schedule (A) paragraph (45) of the Transitional Constitution of South Sudan, 2011 (as amended).

(2) The provisions of this Act shall apply to all cybercrimes and computer misuse committed in or outside the Republic of South Sudan.

5. Interpretations

In this Act, unless the context otherwise requires:

CHAPTER VII
GENERAL PROVISIONS

CHAPTER IV
ESTABLISHMENT OF THE PROSECUTION UNIT AND PROCEDURAL POWERS OF INVESTIGATION

CHAPTER V
CRITICAL NATIONAL INFRASTRUCTURE

CHAPTER VI
OFFENCES AND PENALTIES

LAWS OF SOUTH SUDAN
CYBERCRIMES AND COMPUTER MISUSE ACT, 2026

ARRANGEMENT OF SECTIONS

CHAPTER I
PRELIMINARY PROVISIONS

CHAPTER II
OBLIGATIONS OF SERVICE PROVIDERS AND JURISDICTION OF CYBERCRIMES AND COMPUTER MISUSE ACT.

CHAPTER III
INTERNATIONAL COOPERATION

THE REPUBLIC OF SOUTH SUDAN
LAWS OF SOUTH SUDAN

CYBERCRIMES AND COMPUTER MISUSE ACT, 2026