Commonwealth Countries' Cybercrime Laws

An Overview

The Commonwealth

Commonwealth Countries' Cybercrime Laws

An Overview

The Commonwealth

Foreign, Commonwealth
& Development Office

Commonwealth Secretariat
Marlborough House
Pall Mall
London SW1Y 5HX
United Kingdom

www.thecommonwealth.org

Published by the Commonwealth Secretariat.

Contents

Foreword

Cybercrime is a growing threat to the security, prosperity and well-being of the Commonwealth and its member countries, and poses a challenge to security, privacy, the economy and human rights. Some of these challenges include a lack of harmonised legal frameworks to address the diverse and emergent forms of sophisticated cyberattacks.

Proper cybercrime legislation is key to a comprehensive and holistic approach in addressing the challenges and opportunities of cyberspace. To combat cybercrime effectively, there is a need for coordinated policies and actions at the national, regional and international levels across the Commonwealth and beyond. In line with the common vision set out in the 2018 Commonwealth Cyber Declaration, all member countries are enjoined to ensure that the cyberspace remains free, open and inclusive across the Commonwealth.

Commonwealth member countries are at various cyber-legislation maturity levels and a lack of adequate legal frameworks and cybersecurity strategies implies a vulnerability to cyber threats. Without an appropriate legal framework, cybercrime will increasingly undermine essential trust and confidence in Information Communications Technologies (ICTs) required for achieving the Sustainable Development Goals (SDGs) and advancing the Commonwealth's values of democracy, human rights, rule of law and good governance.

Cybercrime legislation should be flexible and adaptable to cope with the dynamic nature of cybercrime and ICTs. The legislation should also foster innovation and creativity in ICT use for social and economic development, which does not infringe on the rights and interests of others. It is therefore imperative that Commonwealth member countries adopt appropriate cybercrime frameworks that can effectively prevent, investigate, and prosecute cybercrime, as well as protect the rights and interests of victims and witnesses.

This mapping report provides an overview of the current state of cybercrime laws and policies in the 56 Commonwealth countries. It highlights challenges, opportunities and best practices for enhancing cybersecurity and resilience. The report aims to foster dialogue and international cooperation for capacity building and to inspire action among all Commonwealth countries in their efforts to tackle cybercrime.

The harmonisation of cybercrime legislation across the Commonwealth will enable international cooperation and mutual legal assistance in combating cybercrime. Appropriate cybercrime legislation should respect and protect human rights and fundamental freedoms, especially the right to privacy, freedom of expression, access to information and due process of law. Such legislation should comply with the principles of legality, necessity, proportionality and accountability.

The Commonwealth Secretariat will continue to assist member countries to build the foundations of an effective national cybercrime response while promoting stability in cyberspace through laws and policies which are people-centred, and which protect human rights and fundamental freedoms.

Rt Hon. Patricia Scotland KC

Secretary-General of the Commonwealth

Acknowledgments

The Commonwealth Secretariat acknowledges with gratitude the financial support of the United Kingdom Foreign, Commonwealth & Development Office to the Commonwealth Cyber Capability Programme.

This *Overview of National Cybercrime Laws in the Commonwealth* considers relevant provisions of statutes, legislative instruments and administrative regulations relevant to managing cybercrime in Commonwealth countries.

The *Overview of National Cybercrime Laws in the Commonwealth* was authored by Professor Nnenna Ifeanyi-Ajufo, School of Law, University of Bradford, and Vice-Chair, African Union Cyber Security Expert Groups.

This is one of several key publications prepared under the general guidance of Professor Luis Franceschi, Assistant Secretary-General and Senior Director for the Governance and Peace Directorate (GPD) and Dr Tawanda Hondora, Adviser and Head of Rule of Law Section, Governance and Peace Directorate (GPD). Dr Nkechi Amobi, Senior Research Officer, Cyber Capability Programme, GPD, led and co-ordinated the review and editorial process of the report.

Ms Emma Beckles, Programme Officer, GPD, and Mr Shakirudeen Ade Alade, Programme Co-ordinator, GPD, conceptualised this research project and Ms Helene Massaka, Programme Assistant, GPD, provided logistical and administrative support.

The team is particularly grateful to the Commonwealth Secretariat's publications and design team for their leadership and support in producing this report.

About this report

All information in this report was fully up to date at the time of writing in June 2023.

Acronyms and Abbreviations

ASEAN	Association of Southeast Asian States
AU	African Union
CCSCAP	CARICOM Cyber Security and Cybercrime Action Plan
CERT	Computer emergency response team
CMA	Computer Misuse Act
CSIRT	Computer security incident response team
ECA	Electronic Crimes Act
ECOWAS	Economic Community of West African States
ETA	Electronic Transactions Act
ICT	Information communication and technology
INTERPOL	International Criminal Police Organization
IMPACS	Implementation Agency for Crime and Security (CARICOM)
NCSC	National Cyber Security Centre
NCSI	National Cyber Security Index
OAS	Organization of American States
UNODC	United Nations Office on Drugs and Crime
SADC	Southern African Development Community
ITU	International Telecommunication Union

Executive Summary

This mapping report, which is by no means exhaustive, is an illustrative overview of the cybercrime laws in the 56 Commonwealth countries.[1] It considers relevant provisions of statutes, legislative instruments and administrative regulations relevant to cybercrime, including computer misuse, electronic evidence and cybersecurity. The report gives a brief overview of the provisions of the law and applicable sanctions for cybercrimes, such as unauthorised interception of data, cyberstalking, unauthorised access to computer systems, pornography and child pornography.

The aim of this report is to map existing national cybercrime laws, identify gaps in cybercrime legislation, highlight existing cybercrime initiatives and capacity gaps in cybersecurity policy efforts in Commonwealth countries. The report objective goes further to inform capacity building priorities and highlight areas for cybersecurity co-operation and collaboration, including to enhance priorities for technical assistance, mutual legal assistance and information sharing for Commonwealth countries.

While the main objective of this report is to provide an overview of the national cybercrime laws in the Commonwealth, it is important to note that apart from the enactment of national cybercrime legislation, Commonwealth countries must also ensure that the prescribed sanctions for cybercrimes are appropriate and commensurate to the crime to ensure deterrence. It is also necessary to ensure that cybercrime laws are compatible with best practices and that they prioritise the protection of human rights and fundamental freedoms, while employing measures to prevent and combat cybercrime.

Commendably, numerous Commonwealth countries now have regulatory frameworks and are taking measures, such as establishing computer incident response teams (CIRTs),[2] to address cybercrime and cybersecurity challenges. In addition, some are strengthening their international co-operation frameworks through acceding to international instruments such as the Council of Europe Convention on Cybercrime remains relevant[3] and the African Union Convention on Cyber Security and Personal Data Protection.

One of the main obstacles to resolving cybercrime matters in many countries is international co-operation and the inability of many countries to access mutual legal assistance especially for data across borders because they are not parties to relevant cybercrime treaties. This report portrays how diverse cybercrime laws are embedded in differing legal systems and traditions and shows that of the 56 Commonwealth countries, 66 per cent have established a national Cyber Security Incident Response Team (CSIRT); 59 per cent have a relevant strategy or policy on cybersecurity in place; and only 18 per cent are party to the Budapest Convention, the leading framework for international co-operation in dealing with cybercrime. Cybercrime is borderless and consequently effective international co-operation through ratification of international instruments such as the Budapest Convention and other mechanisms is imperative considering the volatile nature of electronic evidence, which requires real-time co-operation and advanced technological skills.

It is important that Commonwealth countries employ more sophisticated tools and approaches to address cybercrime and ensure prompt detection of cyber incidents in their countries. The ratification and domestication of international instruments and standard-setting guidance from the Commonwealth Model Law will further strengthen the cyber legislation harmonisation process throughout the Commonwealth.[4]

While the Information contained in this report is considered to be true and correct at the date of research, changes and evolving circumstances post research and date of publication may impact on the accuracy of the Information.

---

1 Antigua and Barbuda, Australia, The Bahamas, Bangladesh, Barbados, Belize, Botswana, Brunei Darussalam, Cameroon, Canada, Cyprus, Dominica, eSwatini, Fiji, Gabon , The Gambia, Ghana, Grenada, Guyana, India, Jamaica, Kenya, Kiribati, Lesotho, Malawi, Malaysia, Maldives, Malta, Mauritius, Mozambique, Namibia, Nauru, New Zealand, Nigeria, Pakistan, Papua New Guinea, Rwanda, Saint Lucia, Samoa, Seychelles, Sierra Leone, Singapore, Solomon Islands, South Africa, Sri Lanka, St Kitts and Nevis, St Vincent and the Grenadines, Tanzania, Tonga, Trinidad and Tobago, Tuvalu, Uganda, United Kingdom, Togo , Vanuatu, Zambia.

2 National CIRT (ITU), available at: www.itu.int:443/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx (accessed 17 January 2023).

3 Parties/observers to the Budapest Convention and Observer Organisations to the T-CY, available at: www.coe.int/en/web/cybercrime/parties-observers (accessed 17 January 2023).

4 Commonwealth Model Law, available at: https://rm.coe.int/1680303ee1 (accessed 23 January 2023).

Introduction

The security and integrity of computer systems, digital data and networks have grown to be major concerns for states, organisations and people as a result of the development of the information society. Such concerns arise from the fact that malicious acts, such as ransomware, which target computer systems and their networks, have the potential to cause harm to individuals, countries and the global economy.[5] Accordingly, many states and intergovernmental organisations across the world have taken steps to establish legal measures to criminalise and deter malicious acts that affect the integrity, confidentiality, availability and security of digital data and computer systems.

Cyberattacks targeted at Commonwealth countries are motivated by individual criminal interests, espionage, disinformation and, sometimes, political interests. Many members of the Commonwealth are affected by inadequate digital capacity, thereby making such countries prone to cyber threats and attacks from malicious cyber actors. Globally, malware attacks increased to 358 per cent in 2020 compared to 2019. Global cyberattacks also increased by 125 per cent through 2021.[6] The cost of cybercrime is estimated to grow from US$3 trillion in 2015 to US$6 trillion by the year 2025.[7] With increasing cyber threats, governments around the world are compelled to enact legislation to govern the online and digital space in order to reduce the occurrence of cyber-related crimes and protect their citizens.[8] According to the United Nations Conference on Trade and Development (UNCTAD) worldwide resource[9], 80 per cent of the UN member countries have cybercrime legislation, 5 per cent with draft legislation, 13 per cent with no legislation, and 1 per cent with no cybercrime data. Generating accurate an up-to-date statistical data on types, trends, scale and impact of cybercrime is difficult and compounded by underreporting in many jurisdictions and an absence of reporting requirements frameworks.

International Cybercrime Regulation/Instruments

There have been diverse efforts to establish legal frameworks for tackling and policing cybercrime at the international, regional and national levels. This has led to various activities aimed at enhancing co-operation and capacity building to effectively tackle cybercrimes. These efforts have involved the United Nations, Commonwealth Secretariat, Council of Europe, African Union Commission (AUC), Association of Southeast Asian States (ASEAN) and the Shanghai Cooperation Organisation (SCO). At the operational and law enforcement level, INTERPOL plays a vital role in 'building cross-sector partnerships and enabling international law enforcement co-operation and collaboration necessary for policing cybercrimes and mitigating cyber threats'.[10] INTERPOL has also continued to ensure cybersecurity capability development for members.[11] Additionally, the INTERPOL Global Cybercrime Expert Group co-ordinates transnational cybercrime investigations and operations and the production of actionable intelligence in relation to policing cybercrime.

---

5 See Tropina, T. 'Cybercrime: Setting International Standards' in Tikk, E and Kerttunen. (2020), *Routledge Handbook of International Cybersecurity*, Routledge, London, 148.

6 'The Latest 2023 Cyber Crime Statistics', available at: https://aag-it.com/the-latest-cyber-crime-statistics/ (accessed 9 January 2023).

7 *Cybercrime Magazine* (2018), 'Cybercrime to cost the World $10.5 trillion annually By 2025', 21 February, available at: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ (accessed 21 January 2023).

8 *Report on Cybersecurity in SADC and its Implications on Human Rights*, available at: www.techzim.co.zw/wp-content/uploads/2021/10/MISA-Report-on-Cybersecurity-in-SADC-its-implications-on-human-rights.pdf (accessed 15 January 2023).

9 UNCTAD, Cybercrime Legislation Worldwide, available at: https://unctad.org/page/cybercrime-legislation-worldwide (accessed 21 January 2023).

10 'Cybercrime', available at: www.interpol.int/en/Crimes/Cybercrime (accessed 31 January 2023).

11 'Cyber Capabilities Development', available at: www.interpol.int/en/Crimes/Cybercrime/Cyber-capabilities-development (accessed 31 January 2023).

a) United Nations

There have been efforts to advance a harmonised legislation for cross-border, cybercrime through an international response. The United Nations has been championing processes and activities aimed at elaborating an international legal instrument that will criminalise cyber activities based on the agreement of member states and many Commonwealth countries have been involved in the United Nations processes.

The United Nations, through its UN Global Programme on Cybercrime[12] under the auspices of the UN Office on Drugs and Crime (UNODC), has focused on assisting member countries in tackling cyber-related crimes through capacity building and technical assistance. The adoption of United Nations General Assembly Resolution A/RES/53/70 on 'Developments in the field of information and telecommunication in the context of international security'[13] arguably marked the emergence of a cybersecurity agenda for the United Nations. The resolution recognised the benefits of information and communication technology (ICT), but acknowledged the risks related to its misuse and called upon member states to promote at multilateral levels the consideration of existing and potential threats in the field of information security.

Ensuing resolutions and events paved the way for the creation of the Group of Government Experts (commonly referred to as the 'Group of Governmental Experts' or UN GGE) under the auspices of the United Nations to study 'Developments in the Field of Information and Telecommunications in the Context of International Security'. The group later became known as 'the United Nations Group of Governmental Experts (GGE) on Advancing responsible state behaviour in cyberspace in the context of international security'. Six working groups have been established since 2004, including GGE 2019–2021, while the UN GGE framework has been the main forum for states to set and pursue an agenda on responsible state behaviour in cyberspace at the international level. Countries have been selected to participate based on equitable geographical distribution and a number of Commonwealth member countries, notably, the United Kingdom, Canada, Australia, India, Singapore, Kenya, Mauritius and South Africa have been members of the GGEs.[14]

A United Nations mandated working group – the Open-Ended Working Group on 'Developments in the Field of ICTs in the Context of International Security' (OEWG) was further instituted pursuant to General Assembly Resolution 73/27 of 5 December 2018, open to all United Nations member states.

The United Nations General Assembly, through Resolution A/RES/74/247 'Countering the use of information and communications technologies for criminal purposes',[15] decided to establish an open-ended ad hoc intergovernmental committee of experts ('the Ad Hoc Committee on Cybercrime'), which is representative of all regions, to elaborate a comprehensive international convention on countering the use of information and communication technologies for criminal purposes. The open-ended Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes is an intergovernmental committee composed of experts and representatives of all regions mandated with drafting a new cybercrime convention. The convention will take into consideration existing international instruments and efforts at the national, regional and international levels on combatting the use of information and communication technologies for criminal purposes.

b) Council of Europe

The Council of Europe Convention on Cybercrime and its additional protocols ('the Budapest Convention')[16] is the first international treaty on crimes committed via the internet and other computer networks. It was opened for signature in Budapest in November 2001. The Convention on Cybercrime was developed under

12 United Nations Global Programme on Cybercrime, 'Global Programme on Cybercrime', available at: www.unodc.org/unodc/en/cybercrime/global-programme-cybercrime.html (accessed 3 April 2023).
13 United Nations General Assembly A/RES/53/70 4 January 1999, available at: https://digitallibrary.un.org/record/265311?ln=en
14 United Nations, 'Group of Governmental Experts', available at: https://www.un.org/disarmament/group-of-governmental-experts/ (accessed 3 April 2023).
15 United Nations General Assembly A/RES/74/247 N1944028.pdf (un.org)
16 The Convention on Cybercrime of the Council of Europe, available at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561 (accessed 3 April 2023).

the auspices of the Council of Europe; however, at the time of writing it remains the most relevant international agreement on cybercrime and electronic evidence.[17] This convention seeks to harmonise national laws, improve cybercrime investigation techniques and improve international co-operation. It also provides guidance to signatories on the measures needed at the national level to deal with cybercrime, including amendments and additions to substantive law (i.e., to establish cybercrime offences in criminal law) and criminal procedural law (i.e., to establish the procedures for criminal investigations and prosecutions). The convention further provides signatories with guidance on mutual assistance and acts as a mutual legal assistance treaty. Its main objective is 'to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation'.[18] Only ten Commonwealth member countries have ratified the Budapest Convention. The Commonwealth Secretariat is an observer organisation to the Cybercrime Convention Committee.[19]

c) The Commonwealth Secretariat

The Commonwealth Model Law on Computer and Computer Related Crime 2017.[20] The Model Law on Computer and Computer-Related Crime 2002 is aimed at supporting Commonwealth countries in putting in place effective legal frameworks to combat cybercrime. It is an effort by Commonwealth countries to harmonise cybercrime legislation and it serves as a guide to the principles Commonwealth countries can use in developing their cybercrime legislation.

The Commonwealth Cyber Declaration (CCD) 2018.[21] The Declaration was adopted at the Commonwealth Heads of Government Meeting (CHOGM) in London in 2018. Through the instrument of the Declaration, Commonwealth member countries affirm their shared interest in protecting the security of communication networks and data, as well as the people that use them and the services that run on them. The Declaration commits member countries to three core pillars:

- promoting a cyberspace that supports economic and social development and rights online;
- building the foundations of an effective national cybersecurity response; and
- promoting stability in cyberspace through international co-operation. The CCD builds on the principles expressed in the 2014 Commonwealth Cyber Governance Model and emphasises the critical role of cyberspace in connecting all Commonwealth member countries in the context of advancing social and economic development.

Commonwealth Cyber Governance Model 2014.[22] In March 2014, Commonwealth ICT ministers agreed to broad principles of cyber governance linked to The Commonwealth's values. The model recognises the central importance of the internet to Commonwealth countries and sets out principles to guide Commonwealth members in planning and implementing practical actions in policy development, regulation and legislation, cross-border collaboration, capacity building, and technical measures in relation to cyberspace governance.

The Commonwealth Approach for Developing National Cybersecurity Strategies.[23] The Commonwealth Approach for Developing National Cybersecurity Strategies is a guide to creating a cohesive and inclusive approach to delivering a safe, secure and resilient cyberspace. It was developed by the

17 The Budapest Convention on Cybercrime: A Framework for Capacity Building – Global Forum on Cyber Expertise, available at: https://thegfce.org/the-budapest-convention-on-cybercrime-a-framework-for-capacity-building/ (accessed 24 January 2023).
18 Council of Europe, 'Complete list of Council of Europe's treaties', Treaty Office, available at: www.coe.int/en/web/conventions/full-list (accessed 25 January 2023).
19 Council of Europe, Observer Organisations to the Cybercrime Convention Committee, available at: https://www.coe.int/en/web/cybercrime/parties-observers?trk=public_post_comment-text (accessed 3 April 2023).
20 The Commonwealth Model Law on Computer and Computer Related Crime (2017), available at: https://production-new-commonwealth-files.s3.eu-west-2.amazonaws.com/migrated/key_reform_pdfs/P15370_11_ROL_Model_Law_Computer_Related_Crime.pdf
21 The Commonwealth Cyber Declaration (2018), available at: https://thecommonwealth.org/commonwealth-cyber-declaration-2018
22 Commonwealth Cyber Governance Model, Commonwealth ICT Ministers Forum (2014), available at: www.cto.int/wp-content/uploads/2021/09/The-Commonwealth-Cybergovernance-Model.pdf
23 The Commonwealth Approach for Developing National Cybersecurity Strategies, available at: https://www.cto.int/wp-content/uploads/2021/09/Commonwealth-Approach-for-National-Cybersecurity-Strategies.pdf

Commonwealth Telecommunications Organisation (CTO), its members and partners with the objective of designing a framework for the development of national cybersecurity strategies. It provides a framework and guidance for Commonwealth member countries that wish to develop cybersecurity strategies that are aligned to the principles of the Commonwealth.

The Commonwealth of Independent States' Agreement on Cooperation in Combating Offences Related to Computer Information of 2001. The Commonwealth of Independent States (CIS) in 2001 adopted the Agreement on Cooperation in Combating Offences Related to Computer Information. The Agreement calls on states to adopt national laws to implement the Agreement's provisions and harmonise national cybercrime laws.

Regional cybercrime instruments

There are several cybercrime and cybercrime-related treaties and agreements that are region specific and relevant to Commonwealth countries. These include the following:

African Union Convention on Cyber Security and Personal Data Protection 2014. The African Union Convention on Cyber Security and Personal Data Protection 2014 ('the Malabo Convention') was drafted in 2011 to establish a 'credible framework for cyber security in Africa through organisation of electronic transactions, protection of personal data, promotion of cyber security and combating cybercrime'. The African Union (AU) adopted the convention in June 2014. The convention addresses three main areas:

- electronic transactions;
- personal data protection;
- cybersecurity and cybercrime.

The convention encourages AU member states to recognise the need to protect ICT infrastructure, personal data and to encourage free flow of information through a unified regulatory framework on cybersecurity and personal data protection. The convention is yet to enter into force per Article 36 of the convention by reason of inadequate ratifications from the required 15 African states. At the time of writing, only 14 instruments of ratification had been deposited. Seven Commonwealth member countries have ratified the Malabo Convention: The Gambia, Ghana, Mauritius, Namibia, Rwanda, Togo and Zambia.

ASEAN Declaration to Prevent and Combat Cybercrime 2017.[24] Through the Declaration, member states of the Southeast Asian Nations pledged and resolved to strengthen the commitment of ASEAN member states to co-operate at the regional level in preventing and combatting cybercrime. This Declaration included Brunei Darussalam, Malaysia, and the Republic of Singapore, which are Commonwealth member countries.

The Shanghai Cooperation Organization's Agreement on Cooperation in the Field of International Information Security 2010.[25] This Agreement was established to serve as a legal and organisational basis of co-operation of the Shanghai Cooperation Organisation (SCO) in the field of ensuring the security of international information with the aim of limiting threats to international information security. The Agreement's focus can also be interpreted in terms of cybercrime and cybersecurity. It focuses on the information security (INFOSEC) of member states as a primary subject and makes provisions for threats in the field of ensuring international information security.

Sub-regional legal frameworks

There have also been efforts at the sub-regional levels to provide guidance for legal frameworks for combatting cybercrime. These include the Economic Community of West African States (ECOWAS) and the Southern African Development Community (SADC). At the sub-regional level, SADC adopted the SADC Model Law on Cybercrime in 2012 to guide and facilitate the harmonisation of domestic laws on cybercrime, while ECOWAS adopted the Economic Community of West African States (ECOWAS) Directive on Fighting Cybercrime within ECOWAS 2011, which included other independent cyber governance strategies being undertaken by the ECOWAS.

24 ASEAN Declaration to Prevent and Combat Cybercrime (2017), available at: https://asean.org/wp-content/uploads/2017/11/ASEAN-Declaration-to-Combat-Cybercrime.pdf

25 The Shanghai Cooperation Organization's Agreement on Cooperation in the Field of International Information Security, available at: 2010https://cis-legislation.com/document.fwx?rgn=28340

The following section provides an overview of relevant national security policies, strategies and institutional frameworks for combatting cybercrime in the various Commonwealth countries.

National Cybercrime Legal Frameworks

1. Antigua and Barbuda

A. National cyber threat landscape

According to the National Cyber Security Index (NCSI),[26], as of January 2023 Antigua and Barbuda ranked 140th out of 161 countries on the NCSI with a score of 11.69; 142nd out of 194 countries on the Global Cybersecurity Index; and 76th on the ICT Development Index. A cybercrime strategy is however still pending.

B. National cybercrime legislation and related laws

- Electronic Crimes Act 2013[27]
- Electronic Crimes (Amendment) Act 2018[28]
- The Electronic Transfer Of Funds Crimes Act 2006[29]
- Electronic Transactions Act 2006[30]
- Electronic Transactions Act 2013[31]
- Electronic Transactions Act Amendment 2018[32]
- Electronic Evidence Act 2013[33]
- Computer Misuse Act 2006[34]
- Data Protection Act 2013[35]
- The Copyright Act 2003[36]

C. Scope/application of laws

- The Electronic Crimes Act (ECA) 2013 'provides for the prevention and punishment of electronic crimes and for related matters'.[37] Part II of the Act provides for cyber offences such as: unauthorised access and interference with an electronic system or network; identify theft; electronic forgery; electronic fraud; misuse of encryption; child pornography; electronic terrorism; false websites and spam.[38]

---

26 NCSI: Antigua and Barbuda, available at: https://ncsi.ega.ee/country/ag/ (accessed 17 January 2023).
27 Electronic Crimes Act 2013, available at: http://laws.gov.ag/wp-content/uploads/2019/02/a2013-14.pdf (accessed 9th January 2023).
28 Electronic Crimes (Amendment) Act 2018, available at: http://laws.gov.ag/wp-content/uploads/2019/02/No.-25-of-2018-Electronic-Crimes-Amendment-Act-2018.pdf (accessed 9th January 2023).
29 Electronic Transfer of Funds Crimes Act, 2006 , available at: http://www.oas.org/juridico/spanish/cyb_ant_transfer_fund_2006.pdf (accessed 9 January 2023).
30 Electronic Transactions Act 2006, available at: http://laws.gov.ag/wp-content/uploads/2020/02/No.-8-of-2006-The-Electronic-Transactions-Act-1.pdf (accessed 9 January 2023).
31 Electronic Transactions Act 2013, available at: http://laws.gov.ag/wp-content/uploads/2019/04/Electronic-Transactions-Act-2013.pdf (accessed 9 January 2023).
32 Electronic Transactions (Amendment) Act 2016, available at: http://laws.gov.ag/wp-content/uploads/2019/02/a2016-10.pdf (accessed 10 January 2023).
33 Electronic Evidence Act 2013, available at: http://laws.gov.ag/wp-content/uploads/2019/02/a2013-11.pdf (accessed 9 January 2023).
34 Computer Misuse Act 2006, available at: http://www.oas.org/juridico/spanish/cyb_ant_computer_misuse_2006.pdf (accessed 9 January 2023).
35 Data Protection Act 2013, available at: http://laws.gov.ag/wp-content/uploads/2019/02/a2013-10.pdf (accessed 10 January 2023).
36 Copyright Act 2003, available at: https://abipco.gov.ag/wp-content/uploads/2017/07/Copyright-Act-2003-1.pdf (accessed 10 January 2023).
37 Electronic Crimes Act 2013, available at: http://laws.gov.ag/wp-content/uploads/2019/02/a2013-14.pdf (accessed 9 January 2023).
38 Ibid at Part II, section 3-15.

- The Electronic Crimes (Amendment) Act 2018 was enacted to amend the ECA 2013. It amends some provisions of the ECA 2013 that are related to cyber offences, such as sections 2, 6, 7 and 9 on child pornography, electronic forgery, electronic fraud and misuse of encryption, respectively.
- The Electronic Transfer of Funds Crimes Act regulates the transfer of money by electronic means. Part II of the Act covers offences[39] such as fraudulent electronic funds transfer.[40]
- The Electronic Transactions Act 2006 'establishes the legal principles applicable to the conduct of electronic commerce and the processing, verification and attribution of electronic records'.
- The Electronic Transactions Act (ETA) 2013 was enacted to 'give legal effect to electronic documents, records, and signatures and for incidental and connected purposes'.
- The Electronic Transactions (Amendment) Act 2018 amends section 31 of the ETA 2013, by repealing subsection (2) of the section.
- The Electronic Evidence Act 2013 makes provision for 'the legal recognition of electronic records and to facilitate the admission of such records into legal proceedings and other related matters'.
- The Computer Misuse Act 2006 was enacted 'to prohibit the unauthorised access, use of or interference to any program or data held in a computer and to a computer itself and to facilitate the gathering and use of electronic evidence'. It provides for cyber-related offences such as: unauthorised access to a computer program or data,[41] unauthorised use or interception of computer service,[42] identity theft[43] and child pornography[44].
- The Data Protection Act 2013 'promotes the protection of personal data processed by public and private bodies and for incidental and connected purposes'.

D. Sanctions/penalties

- Section 27 of the ECA 2013 provides for the general penalty for a body corporate as: a fine not exceeding 200,000 dollars or to a term of imprisonment not exceeding three years, or to both; or a fine not exceeding 500,000 dollars or to a term of imprisonment not exceeding eight years, or to both; for summary conviction and conviction on indictment respectively. Also, section 29 makes a person convicted under the Act to be liable to pay compensation for damage caused. Further, the court may also order the forfeiture of the thing 'which is the subject matter of the offence or is used in connection with the commission of the offence'.[45]
- The Electronic Crimes (Amendment) Act 2018 prescribes punishment for cyber offences such as electronic forgery, electronic fraud, with terms of imprisonment ranging between two to seven years, and a fine from 200,000 dollars to 500,000 dollars, or both imprisonment and a fine.[46]

---

39 Electronic Transfer of Funds Crimes Act 2006, section 3–18, available at: www.oas.org/juridico/spanish/cyb_ant_transfer_fund_2006.pdf (accessed 9 January 2023).

40 Electronic Transfer of Funds Crimes Act 2006 , section 19, available at: http://www.oas.org/juridico/spanish/cyb_ant_transfer_fund_2006.pdf (accessed 9 January 2023).

41 Computer Misuse Act 2006, section 3, available at: www.oas.org/juridico/spanish/cyb_ant_computer_misuse_2006.pdf (accessed 9 January 2023).

42 Ibid, section 6.

43 Ibid, section 14.

44 Ibid, section 15.

45 Electronic Crimes Act, 2013, section 30, available at: http://laws.gov.ag/wp-content/uploads/2019/02/a2013-14.pdf (accessed 9 January 2023).

46 Electronic Crimes (Amendment) Act 2018, sections 5 and 6, available at: http://laws.gov.ag/wp-content/uploads/2019/02/No.-25-of-2018-Electronic-Crimes-Amendment-Act-2018.pdf (accessed 9th January 2023).

- The Electronic Transfer of Funds Crimes Act prescribes the sanction for fraudulent electronic fund transfer as: 'summary conviction to a fine of 30,000 dollars or to imprisonment for two years or to both; or conviction on indictment to a fine of 50,000 dollars or to imprisonment for five years or to both'.[47]
- The Electronic Transactions Act 2013 prescribes the penalty for an offence under the Act as: 'summary conviction to a fine not exceeding 200,000 dollars or to imprisonment for a term not exceeding three years; or conviction on indictment to a fine not exceeding 500,000 dollars or to imprisonment for a term not exceeding six years'. For a body corporate, the court can may also impose a fine up to ten per cent of the last audited year of the enterprise.[48]
- The Computer Misuse Act (CMA) prescribes sanctions for offence committed under the Act, with liability ranging from a fine of 15,000 to 250,000 dollars, or imprisonment from two to ten years, or to both fine and imprisonment.[49]

E. National computer emergency response team (CERT)/computer security incident response team (CSIRT)
Antigua and Barbuda does not have a functional computer security incident response team (CSIRT) that provides a 24/7 co-ordinated emergency response to cybersecurity threats.

F. National cybersecurity strategy
Antigua and Barbuda is yet to officially complete a national cybersecurity strategy.

G. Initiatives to combat cybercrime
- Antigua and Barbuda is a member of the Caribbean Community (CARICOM), which focuses on integration and co-operation on areas such as trade, criminal justice, the environment and technical standards among its member states.[50] CARICOM operates through autonomous institutions such as the CARICOM Implementation Agency for Crime and Security (IMPACS),[51] which provides security strategies and responds to issues of crime and security. The member states also signed off on the CARICOM Cyber Security and Cybercrime Action Plan (CCSCAP)[52] in 2017. IMPACS helps member states address threats and vulnerabilities by codifying a 'practical, harmonised standard of practices, systems and expertise for cybersecurity, to which each Caribbean country could aspire'. In 2019, the organisation's objectives were given a boost when it secured funding from the European Union to undertake a 'capacity development' project across CARICOM nations.[53]
- Antigua and Barbuda is one of the 195 International Criminal Police Organization (INTERPOL)[54] member countries.[55] Antigua and Barbuda relies on INTERPOL for training and co-operation in the absence of a National CSIRT.

---

47 Electronic Transfer of Funds Crimes Act 2006, section 19, available at: www.oas.org/juridico/spanish/cyb_ant_transfer_fund_2006.pdf (accessed 9 January 2023).
48 Electronic Transactions Act 2013, section 40, available at: http://laws.gov.ag/wp-content/uploads/2019/04/Electronic-Transactions-Act-2013.pdf (accessed 9 January 2023).
49 Part II Computer Misuse Act 2006, available at: www.oas.org/juridico/spanish/cyb_ant_computer_misuse_2006.pdf (accessed 9 January 2023).
50 PublicTechnology.net (2022), 'No one is an island: how Caribbean states are working together to tackle cybercrime', 17 October, available at: https://publictechnology.net/articles/features/no-one-island-how-caribbean-states-are-working-together-tackle-cybercrime (accessed 24 January 2023).
51 CARICOM Implementation Agency for Crime and Security, available at: https://caricomimpacs.org/about-us-v1/ (accessed 27 January 2023).
52 CARICOM Cyber Security and Cybercrime Action Plan, available at: https://caricomimpacs.org/wp-content/uploads/2020/11/CARICOM-Cyber-Security-and-Cybercrime-Action-Plan.pdf (accessed 27 January 2023).
53 PublicTechnology.net (2022), 'No one is an island: how Caribbean states are working together to tackle cybercrime', 17 October, available at: https://publictechnology.net/articles/features/no-one-island-how-caribbean-states-are-working-together-tackle-cybercrime (accessed 24 January 2023).
54 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
55 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).

- The Government of Antigua and Barbuda also has initiatives to create cyber awareness among its populace. One such initiative is the 'AntiguaRecon'[56] Cyber Security initiative, which offers cybersecurity training for students. There is also the 'online platform for learning ethical hacking skills through gamified hands-on training modules'.[57]
- The Government, through the Ministry of Information, Broadcasting, Telecommunications and Information Technology, has also been known to organise awareness programmes such as having a dedicated cybersecurity month to sensitise the public on the importance of cybersecurity.[58]
- There are bodies such as the National Cyber Security Alliance (NCSA) and the Anti-Phishing Working Group (APWG),[59] which provide a response to cybercrime and detection of cyber incidents.
- The STOP THINK CONNECT[60] initiative is another way the importance of cybersecurity awareness and best practices when using the internet are spread in the country. This is an online initiative through which 'tips on how to keep a clean machine from malware and other online threats, protect your personal information when using Wi-Fi hotspot or an open internet connection, customising privacy and security setting on social media and other information are shared'.[61]

2. Australia

A. National cyber threat landscape

According to the National Cyber Security Index (NCSI),[62] as of January 2023 Australia ranked 39th out of 161 countries on the NCSI with a score of 66.23; 12th out of 194 countries on the Global Cybersecurity Index; and 14th on both the ICT Development Index and the Networked Readiness Index. Further, statistics reveal that 'on average, there is a cyberattack every 10 minutes in Australia. From July 2021 to June 2022, cyberattack in Australia increased by 81%'.[63] Australia has also been at the forefront of international co-operation initiatives aimed at promoting cybersecurity.

B. National cybercrime legislation and related laws

- Criminal Code Act No. 12 of 1995[64]
- Cybercrime Act No. 161 of 2001[65]
- The Cybercrime Legislation Amendment Act No.120/2012[66]
- Telecommunications Act 1997[67]

56 Antiguarecon, Home, available at: www.antiguarecon.com (accessed 1 February 2023).
57 Michael, V (2021), 'High school students encouraged to sign up for e-sports initiative', *Antigua Observer Newspaper*, 14 December, available at: https://antiguaobserver.com/high-school-students-encouraged-to-sign-up-for-e-sports-initiative/ (accessed 25 January 2023).
58 Cybil Portal (2022), 'Canadas support to the OAS and its member states in addressing the gender gap in the cybersecurity agenda', 19 December, available at: https://cybilportal.org/projects-by/ (accessed 1 February 2023)
59 APWG, Unifying the global response to cybercrime, available at: https://apwg.org/ (accessed 1 February 2023)
60 Stop Think Connect, available at: www.stopthinkconnect.org.ag (accessed 7 January 2023).
61 Government of Antigua and Barbuda, available at: https://ab.gov.ag/media_page.php?page=181 (accessed 25 January 2023).
62 NCSI: Antigua and Barbuda, available at: https://ncsi.ega.ee/country/ag/ (accessed 17 January 2023).
63 'The Latest 2023 Cyber Crime Statistics', available at: https://aag-it.com/the-latest-cyber-crime-statistics/ (accessed 9 January 2023).
64 Criminal Code Act 1995, available at: www.legislation.gov.au/Details/C2021C00183/Html/Volume_1, http://www.legislation.gov.au/Details/C2021C00183 (accessed 17 January 2023).
65 Cybercrime Act 2001, available at: www.legislation.gov.au/Details/C2004C01213/Html/Text, http://www.legislation.gov.au/Details/C2004C01213 (accessed 17 January 2023).
66 Cybercrime Legislation Amendment Act 2012, available at: www.legislation.gov.au/Details/C2012A00120/Html/Text, http://www.legislation.gov.au/Details/C2012A00120 (accessed 17 January 2023).
67 Telecommunications Act 1997, available at: www.legislation.gov.au/Details/C2022C00170/Html/Volume_1, http://www.legislation.gov.au/Details/C2022C00170 (accessed 17 January 2023).

- Telecommunications (Interception and Access) Act 1979[68]
- At the state level, New South Wales has enacted the Crimes Act 1900,[69] Surveillance Devices Act 2007[70] and the Crimes (Domestic and Personal Violence) Act 2007[71]
- The Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018[72]

C. Scope/application of laws

- The Criminal Code Act criminalises the misuse of telecommunication networks, carriage services and computers. It provides for cyber offences such as dealing in identification information that involves use of a carriage service;[73] use of a carriage service for child abuse material; unauthorised access, modification or impairment with intent to commit a serious offence; unauthorised impairment of electronic communication; unauthorised access to, or modification of, restricted data; and possession or control of data with intent to commit a computer offence. Cybercrime offences are found in Commonwealth legislation within parts 10.7 and 10.8 of the Criminal Code Act 1995 and include: computer intrusions; unauthorised modification of data, including destruction of data; unauthorised impairment of electronic communications, including denial of service attacks; the creation and distribution of malicious software (for example, malware, viruses, ransomware); and dishonestly obtaining or dealing in personal financial information.
- The Cybercrime Act 2001 amends the law (criminal code) relating to computer offences and other related purposes. It inserts part 10.7, which provides for computer offences, reiterates the provisions of Divisions 477 and 478 on serious computer offences and other offences, and provides law enforcement powers relating to electronically stored data.
- The Cybercrime Legislation Amendment Act implements the Council of Europe Convention on Cybercrime and other related purposes. It further repeals and amends provisions of the Criminal Code 1995, the Telecommunications Act 1997, Mutual Assistance in Criminal Matters Act 1987 and the Telecommunications (Interception and Access) Act 1979.
- The Telecommunications Act provides a framework for the telecommunications industry, and the provision of carriage services.
- The Telecommunications (Interception and Access) Act prohibits the interception of, and other access to, telecommunications, except where authorised in special circumstances.

D. Sanctions/penalties

- Under the Criminal Code Act, conviction for unauthorised modification of data to cause impairment or unauthorised impairment of electronic communication attracts a penalty of 10 years imprisonment.[74] Other computer offences under Division 478 of the Act attract between two and three years' imprisonment.

---

68 Telecommunications (Interception and Access) Act 1979, available at: www.legislation.gov.au/Details/C2023C00005/Html/Text, http://www.legislation.gov.au/Details/C2023C00005 (accessed 17 January 2023).

69 NSW Legislation, available at: https://legislation.nsw.gov.au/view/html/inforce/current/act-1900-040 (accessed 17 January 2023).

70 NSW Legislation, available at: https://legislation.nsw.gov.au/view/whole/html/inforce/current/act-2007-064 (accessed 17 January 2023).

71 NSW Legislation, available at: https://legislation.nsw.gov.au/view/whole/html/inforce/current/act-2007-080 (accessed 17 January 2023).

72 Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018, available at: www.legislation.gov.au/Details/C2021C00496/Html/Text, http://www.legislation.gov.au/Details/C2021C00496 (accessed 17 January 2023).

73 Criminal Code Act 1995, section 372.1A, available at: http://www.legislation.gov.au/Details/C2021C00183/Html/Volume_2 (accessed 17 January 2023).

74 Ibid, section 477.2 and section 477.3.

E. National computer emergency response team (CERT)/computer security incident response team (CSIRT)
Australia CERT ('AusCERT')[75] is tasked with preventing, detecting, responding and mitigating cyber-based attacks in the country.

F. National cybersecurity strategy
- Implementation of the National Plan to Combat Cybercrime in 2022,[76] with the aim to build Australia's resilience to cybercrime.
- The 2020 Cyber Security Strategy builds on the country's 2016 Cyber Security Strategy, which invested $230 million Australian dollars to advance and protect Australia's interests online. The vision of the 2020 strategy is to build a 'more secure online world for Australians, their businesses and the essential services upon which we all depend'.[77] The vision is to be carried out by government, businesses and the community through actions such as: sharing threat information, strengthening cybersecurity partnerships, enhancing cybersecurity capabilities, improving baseline security for critical infrastructure and reporting cybercrime. [78]

G. Initiatives to combat cybercrime
- Australia ratified the Convention on Cybercrime (ETS No. 185)[79] on 30 November 2012. It came into effect in the country on 1 March 2013.[80]
- Implementation of the 2022 National Plan to Combat Cybercrime[81] became necessary to deal with problems which the 2013 National Plan to Combat Cybercrime did not envisage.[82] The national plan 'builds on the actions of the Commonwealth, state and territory governments, including initiatives delivered under Australia's Cyber Security Strategy 2020, the National Strategy to Fight Transnational, Serious and Organised Crime, the Ransomware Action Plan, the National Strategy to Prevent and Respond to Child Sexual Abuse,'[83] and aims to build Australia's resilience to cybercrime.
- Implementation of the country's 2020 Cyber Security Strategy.[84]
- Australia is one of the 195 INTERPOL[85] member countries.[86] The Australian Federal Police also works closely with state and territory police and international policing agencies in the fight against all types of cybercrime.
- Provision of funds to combat cybercrimes: The government, on 6 August 2020 through the Minister for Home Affairs while giving the foreword to the 2020 Cybersecurity Strategy, stated its intention to provide sufficient funds to the implementation of the country's Cybersecurity Strategy. It committed to invest '$1.67 billion over ten years in cyber security'

75 AusCERT, Home, available at: https://auscert.org.au/ (accessed 17 January 2023).
76 National Plan to Combat Cybercrime 2022, available at: www.homeaffairs.gov.au/criminal-justice/files/national-plan-combat-cybercrime-2022.pdf (accessed 17 January 2023).
77 Cyber Security Strategy, available at: www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf> accessed 17 January 2023).
78 Ibid.
79 Council of Europe, 'The Budapest Convention (ETS No. 185) and its Protocols', available at: www.coe.int/en/web/cybercrime/the-budapest-convention (accessed 26 January 2023).
80 Council of Europe, 'Complete list of Council of Europe's treaties', Treaty Office, available at: www.coe.int/en/web/conventions/full-list (accessed 25 January 2023).
81 National Plan to Combat Cybercrime 2022, available at: www.homeaffairs.gov.au/criminal-justice/files/national-plan-combat-cybercrime-2022.pdf (accessed 17 January 2023).
82 National Plan to Combat Cybercrime, available at: www.homeaffairs.gov.au/criminal-justice/files/national-plan-combat-cybercrime.pdf (accessed 9 January 2023).
83 Ibid.
84 Cyber Security Strategy, available at: www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf (accessed 17 January 2023).
85 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
86 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).

in the country.[87] There is also the A$30.9 million invested over three years under the National Cybercrime Capability Fund to uplift the capability of Commonwealth and state and territory law enforcement agencies to combat cybercrime.[88]

- Innovative initiatives in tackling cybercrime such as: establishment of the Cyber Security Centre's ReportCyber,[89] which enables the populace to report and refer cybercrimes to law enforcement agents;[90] opening the Australian Cyber Security Centre (ACSC); establishing a 24/7 global watch on cyber threats; providing support – 'IDCARE' – to victims of cybercrime;[91] creating an office and appointing an ambassador for cyber affairs and critical technology; establishing the Office of the eSafety Commissioner; creation of a 24/7 cybersecurity advice hotline for small and medium-sized enterprises (SMEs) and families; and establishing the Australian Cybersecurity Growth Network and the Cybersecurity Co-Operative Research Centre. The ACSC leads on national cybersecurity. It brings together cybersecurity capabilities from across the Australian Government to improve the cyber resilience of the Australian community and support the economic and social prosperity of Australia in the digital age. It also facilitates comprehensive understanding of cyber threats and provides advice and assistance to help Australians identify and manage cyber risk. The ACSC includes staff from the Australian Federal Police and Australian Signals Directorate, Department of Home Affairs, Australian Criminal Intelligence Commission and Australian Security Intelligence Organisation.
- Joint Cyber Security Centres (JCSCs) have opened in Brisbane, Melbourne, Sydney, Perth and Adelaide, to bring together the business and research communities along with state, territory and Commonwealth agencies to enhance collaboration on cybersecurity. JCSCs are a critical hub for business and governments to improve their cybersecurity practices and share information in a trusted and secure environment.
- Establishment of Joint Cyber Security Centres (JCSCs) to engage state and territory governments and industry on ways to combat cybercrime.
- Development of a Cyber and Critical Technology International Engagement Strategy to 'provide a framework to guide Australia's international engagement, ensure cyberspace and critical technology, and support our goal of a safe, secure and prosperous Australia, Indo-Pacific and world'.[92] This flows from the success of the 2017 International Cyber Engagement Strategy.[93] Under the strategy, 'Australia invests $AU74 million towards international co-operation initiatives to support Southeast Asia and the Pacific to strengthen their resilience, including specific projects to build capacity in cybercrime prevention and prosecution'.[94]
- Apart from the substantive cybercrime legislations, enacting legislations such as the Surveillance Legislation Amendment (Identify and Disrupt) Act 2021 (SLAID Act) to 'enhance the ability of the Australian Criminal Intelligence Commission (ACIC) and AFP to

87 Ibid.
88 2022 National Plan to Combat Cybercrime, available at: www.homeaffairs.gov.au/criminal-justice/files/national-plan-combat-cybercrime-2022.pdf (accessed 25 January 2023).
89 ReportCyber, Cyber Security Centres, available at: www.cyber.gov.au/acsc/report (accessed 17 January 2023).
90 Almost 500 ransomware-related cybercrime reports were received via the ReportCyber website in the 2020–21 financial year.
91 As part of Australia's Cyber Security Strategy 2020, the Australian government has committed AU$6.1 million towards IDCARE to support Australians impacted as victims of cybercrime.
92 Cyber Security Strategy, available at: www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf (accessed 17 January 2023).
93 International Cyber Engagement Strategy, available at: www.internationalcybertech.gov.au/sites/default/files/2020-11/The%20Strategy.pdf (accessed 28 January 2023).
94 Cyber Security Strategy, available at: www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf (accessed 17 January 2023).

discover, target, investigate and disrupt serious criminal activity occurring online';[95] and the Online Safety Act 2021, which 'places safety at the heart of how Australians navigate the online world by providing more powers for the eSafety Commissioner'.[96]

3. The Bahamas

A. National cyber threat landscape

According to the National Cyber Security Index (NCSI),[97] as of January 2023 The Bahamas ranked: 119th out of 161 countries on the NCSI with a score of 20.78; 147th out of 194 countries on the global Cybersecurity Index; and 57th on the ICT Development Index. An increase has been reported in cybercrime rates in The Bahamas, with a report revealing that 'between January 1st and June 30th, 2020, there were 118 cybercrime incidents reported to authorities, compared to the 87 matters reported during the same period in 2019'.[98]

B. National cybercrime legislation and related laws

- Computer Misuse Act 2003[99]
- Electronic Communications and Transactions Act 2003[100]
- Data Protection (Privacy of Personal Information) Act 2003[101]
- Bahamas National Crime Intelligence Agency Act 2019[102]
- Criminal Procedure Code[103]

C. Scope/application of laws

- The Computer Misuse Act (CMA) is the only Bahamian legislation that addresses cybercrime directly. It makes provisions securing computer material against unauthorised access or modification and for connected purposes. It specifically provides for offences such as: unauthorised access to computer material;[104] unauthorised modification of computer material;[105] unauthorised use or interception of a computer service;[106] unauthorised disclosure of an access code, incitement, abetment and attempt; and relevant law enforcement powers.[107] Apart from criminalising the most common forms of cybercrime, the CMA also covers offences such as cyberstalking, cyberbullying, unlawful online gaming and online prostitution.
- The Electronic Communications and Transactions Act provides for: 'The legal recognition of electronic writing, electronic contracts, electronic signatures and original information in electronic form in relation to commercial and other transactions and to provide for the facilitation of electronic transactions and related matters.'

95 2022 National Plan to Combat Cybercrime, available at: www.homeaffairs.gov.au/criminal-justice/files/national-plan-combat-cybercrime-2022.pdf (accessed 25 January 2023).
96 Ibid.
97 NCSI: The Bahamas, available at: https://ncsi.ega.ee/country/bs/ (accessed 17 January 2023).
98 'Increase in cyber-crime reports in The Bahamas', available at: www.cfatf-gafic.org/home/what-s-happening/664-increase-in-cyber-crime-reports-in-the-bahamas (accessed 17 January 2023).
99 Computer Misuse Act, available at: http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/2003/2003-0002/ComputerMisuseAct_1.pdf (accessed 13 January 2023).
100 Electronic Communications and Transactions Act, available at: http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/2003/2003-0004/ElectronicCommunicationsandTransactionsAct_1.pdf (accessed 31 January 2023).
101 Data Protection (Privacy of Personal Information) Act, available at: http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/2003/2003-0003/DataProtectionPrivacyofPersonalInformationAct_1.pdf (accessed 13 January 2023).
102 National Crime Intelligence Agency Act, available at: http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/2019/2019-0022/NationalCrimeIntelligenceAgencyAct2019_1.pdf (accessed 13 January 2023).
103 Criminal Procedure Code, available at: http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/1968/1968-0038/CriminalProcedureCodeAct_1.pdf (accessed 23 January 2023).
104 Computer Misuse Act, section 3, available at: http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/2003/2003-0002/ComputerMisuseAct_1.pdf (accessed 13 January 2023).
105 Ibid, section 5.
106 Ibid, section 6.
107 Ibid, section 8.

- The Data Protection (Privacy of Personal Information) Act protects and provides for the privacy of individuals with respect to the collection, processing, keeping, use and disclosure of personal data. The Act also contains provisions on privacy, data protection, data subject rights, enforcement and penalties. It also contains exemptions for the transfer of data for criminal investigations and prosecutions and permits international transfers of criminal evidence, including when the transfer is pursuant to treaty.

D. Sanctions/penalties for cyber–related crimes
- Any person guilty of an offence under the Computer Misuse Act shall be liable on summary conviction to a fine not exceeding 10,000 Bahamian dollars or to imprisonment between one and three years or to both such fine and imprisonment; and in the case of a second or subsequent conviction, to a fine not exceeding 20,000 dollars or to imprisonment for a term between three and five years or to both such fine and imprisonment. However, where it involves a protected computer, the person shall be liable on conviction to a fine not exceeding 100,000 dollars or to imprisonment for a term not exceeding 20 years or to both such fine and imprisonment.

E. National computer emergency response team (CERT)/computer security incident response team (CSIRT)
The Bahamas Computer Incident Response Team (CIRT) serves as a focal point for co-ordinating cybersecurity incident response to cyberattacks, and providing cybersecurity support services to government, private organisations and Bahamian citizens.[108]

F. National cybersecurity strategy
The Bahamas has not yet adopted a national cybercrime strategy. However, the CARICOM Cyber Security and Cybercrime Action Plan (CCSCAP) addresses cyber threats facing Caribbean Community (CARICOM) countries. A National Cyber Security Strategy was initially announced for late 2020;[109] however, that strategy is yet to be finalised.

G. Initiatives to combat cybercrime
- The Bahamas is a member of the Caribbean Community (CARICOM).
- The Bahamas is one of the 195 INTERPOL[110] member countries.[111] The Royal Bahamas Police Force (RBPF) also created a dedicated Cyber Security Unit in 2018.
- A specialised cyber security division has been created in the Royal Bahamas Police Force (RBPF).[112] The unit has specially trained cyber investigators and forensics specialists.[113]

4. Bangladesh

A. National cyber threat landscape
Bangladesh ranks first in South Asia in the National Cyber Security Index. According to the NCSI,[114] as of January 2023 Bangladesh ranked: 34th out of 161 countries on the NCSI with a score of 67.53; 53rd out of 194 countries on the Global Cybersecurity Index; 147th on the ICT Development Index; and 95th on the Networked Readiness Index.

---

108 *Our News* (2022), 'PM offers remarks at CIRT Symposium', 24 August, available at: https://ournews.bs/pm-offers-remarks-at-cirt-symposium/ (accessed 17 January 2023).
109 Council of Europe Octopus Community, available at: www.coe.int/en/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/bahamas?_101_INSTANCE_CmDb7M4RGb4Z_viewMode=view/ (accessed 17 March 2023).
110 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
111 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).
112 Royal Bahamas Police Force, Home, available at: www.royalbahamaspolice.org/ (accessed 1 February 2023).
113 Council of Europe, 'Octopus Cybercrime Community', Asset Publisher, available at: www.coe.int/en/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/bahamas/pop_up (accessed 25 January 2023).
114 NCSI: Bangladesh, available at: https://ncsi.ega.ee/country/bd/ (accessed 17 January 2023).

B. National cybercrime legislation and related laws
- National Digital Security Laws (Act No. 46/2018)[115]
- Bangladesh Information and Communication Technology (ICT) Act[116]

C. Scope/application of laws
- The National Digital Security Laws was enacted to ensure digital security in the country, and to enact laws regarding digital crime identification, prevention, suppression, trial and other related matters. It further provides for offences such as: illegal 'entrance' or access to a computer, digital forgery, digital fraud, identity fraud, cyber terrorism,[117] and hacking.[118]
- The Bangladesh Information and Communication Technology (ICT) Act provides legal recognition and security for information and communication technology. It provides for the use of electronic signature and prescribes offences such as: unauthorised access to computer systems, networks or databases;[119] tampering with computer source codes;[120] illegal access or hacking a computer system; and publishing fake,[121] obscene or defaming information in electronic form.[122]

D. Sanctions/penalties for cyber-related offences
- Chapter 6 of the National Digital Security Laws provides for penalties and offences. For instance, section 18 of the Act provides for the illegal 'entrance' or access to a computer, digital device or computer system, and prescribes punishment of imprisonment for a term not exceeding six months or by a fine not exceeding three lakh taka or with both; but with imprisonment not exceeding three years or with a fine not exceeding ten lakh taka when such illegal access was committed with the intention to commit a crime, or on a secured computer system or network.
- If any person commits an offence under the ICT Act, such shall be punishable with imprisonment for a term from three to ten years, or with a fine from one lakh to ten lakh taka, 10,000 taka, or with both a fine and imprisonment.

E. National computer emergency response team (CERT)/computer security incident response team (CSIRT)

The Bangladesh national computer emergency response team is the Bangladesh Government's e-Government Computer Incident Response Team (BGD e-GOV CIRT), which serves as the national CIRT of Bangladesh (N-CIRT). It works as a focal point for Bangladesh for trans-border cyber issues and provides guidance on security threats and vulnerabilities. Its responsibilities include receiving, reviewing and responding to computer security incidents and activities. The team works with various government agencies, critical information infrastructures (CII) stake-holders, financial organisations, law enforcement agencies (LEAs), academia and civil society and has also intensified collaboration efforts with international partners to promote cybersecurity in Bangladesh.[123]

115 National Digital Security Laws, available at: http://www.ilo.org/dyn/natlex/docs/ELECTRONIC/110029/136713/F-353501944/BGD110029.pdf (accessed 13 January 2023).
116 Bangladesh Information and Communication Technology (ICT) Act, available at: https://samsn.ifj.org/wp-content/uploads/2015/07/Bangladesh-ICT-Act-2006.pdf (accessed 13 January 2023).
117 National Digital Security Laws, section 27, available at: http://www.ilo.org/dyn/natlex/docs/ELECTRONIC/110029/136713/F-353501944/BGD110029.pdf (accessed 13 January 2023).
118 Ibid, section 34.
119 Bangladesh Information and Communication Technology (ICT) Act, section 54, available at: https://samsn.ifj.org/wp-content/uploads/2015/07/Bangladesh-ICT-Act-2006.pdf (accessed 13 January 2023).
120 Ibid, section 55.
121 Ibid, section 56.
122 Ibid, section 57.
123 BGD E-GOV CIRT, Bangladesh e-Government Computer Incident Response Team, available at: www.cirt.gov.bd/ (accessed 17 January 2023).

F. National cybersecurity strategy

In terms of the national cybersecurity strategy of Bangladesh,[124] the Digital Security Agency under the Information and Communication Technology (ICT) Division drafted the Bangladesh Cybersecurity Strategy for 2021–2025. The ICT Division placed the strategy before the cabinet for approval in 2022.The first of its kind in Bangladesh, the draft cybersecurity strategy states that all ministries will be equipped with specific software and skilled manpower to protect themselves from cyberattacks. The strategy is part of the moves of the government to ensure the presence 'of long-term measures for protecting the country's cyber world against security threats, risks and challenges to national security'. It creates a coherent vision for keeping the country 'secure and prosperous by co-ordinating government, private sector, citizens and international cyberspace defence efforts'. It further 'outlines a framework for organising and prioritising efforts to manage risks to our cyberspace or critical information infrastructure'.[125]

G. Initiatives to curb cybercrime

- Bangladesh is one of the 195 INTERPOL[126] member countries.[127]
- Creation of a Cyber Tribunal and Cyber Appellate Tribunal[128] pursuant to Chapter 8 of the ICT Act.[129] The tribunal helps to adjudicate cybercrimes and related offences in the country.
- The government has also set up agencies such as: cybercrime prevention agencies like the Bangladesh Telecommunication Regulatory Commission (BTRC)[130] and the Computer Security Incident Response team for Bangladesh (bdCERT),[131] which can help to prevent or reduce incidences of cyber threats.
- Creation of specialised units to fight and investigate cybercrimes and other related offences. These include: 'a cybercrime investigation cell'[132] and 'IT Crime Forensic Lab' in specialised cybercrime police stations.[133]
- Adoption of a National ICT Policy in 2009[134] and implementation of the Bangladesh Cybersecurity Strategy[135] to provide the framework for organising and prioritising efforts to manage risks to the country's cyberspace or critical information infrastructure.
- International collaboration and co-operation with bodies such as the International Telecommunication Union–IMPACS[136] to co-ordinate cybersecurity training.

---

124 National cybersecurity strategy of Bangladesh, available at: https://sherloc.unodc.org/cld/uploads/res/lessons-learned/the_national_cybersecurity_strategy_of_bangladesh_html/The_National_Cybersecurity_Strategy_of_Bangladesh.pdf (accessed 13 January 2023).

125 Ibid.

126 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).

127 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).

128 CyberLaw, the Bangladesh Perspective, available at: http://www.academia.edu/4225890/Cyber_Law_Bangladesh_Perspective (accessed 16 January 2023).

129 Bangladesh Information and Communication Technology (ICT) Act, available at: https://samsn.ifj.org/wp-content/uploads/2015/07/Bangladesh-ICT-Act-2006.pdf (accessed 13 January 2023).

130 Bangladesh Telecommunication Regulatory Commission (BTRC), available at: http://www.btrc.gov.bd/ (accessed 23 January 2023).

131 BGD E-GOV CIRT, Bangladesh e-Government Computer Incident Response Team, available at: www.cirt.gov.bd/ (accessed 17 January 2023).

132 Available at: http://http/www.police.gov.bd/unitscontent.php?id=281 (accessed 16 January 2023).

133 Available at: http://http/www.police.gov.bd/unitscontent.php?id=281 (accessed 16 January 2023).

134 National ICT Policy, available at: https://ictd.gov.bd/site/page/http%3A%2F%2Fictd.gov.bd%2Fsite%2Fpage%2Fafc77b3b-33e5-4a27-b453-6c48a9fe61f8 (accessed 1 February 2023).

135 National Cybersecurity Strategy of Bangladesh, available at: https://sherloc.unodc.org/cld/uploads/res/lessons-learned/the_national_cybersecurity_strategy_of_bangladesh_html/The_National_Cybersecurity_Strategy_of_Bangladesh.pdf (accessed 13 January 2023).

136 ITU (2016), ICB4PAC Project, available at: http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/ICB4PAC/Pages/default.aspx (accessed 15 January 2023).

5. Barbados

A. National cyber threat landscape

According to the National Cyber Security Index (NCSI),[137] as of January 2023 Barbados ranked: 123rd out of 161 countries on the NCSI with a score of 19.48; 139th out of 194 countries on the Global Cybersecurity Index; and 44th on the ICT Development Index.

B. National cybercrime legislation and related laws

- Computer Misuse Act 2005[138]
- Telecommunications Act 2001[139]

C. Scope/application of laws

- The Computer Misuse Act makes provision for the protection of computer systems and the information contained in those systems from: unauthorised access by individuals; abuse by individuals with authorised access; and other related matters. It specifically provides for cyber offences such as: unauthorised modification of a computer program or data,[140] child pornography[141] and unauthorised interception of computer services.[142]
- The Telecommunications Act provides a framework for the management and regulation of the telecommunications network. It creates offences such as unlawful interceptor access and unlawful interference with the telecommunications network or services.

D. National computer emergency response team (CERT)/computer security incident response team (CSIRT)

Barbados is currently in the process of implementing a national computer emergency response team (CERT) in partnership with ITU. ITU is primarily assisting in assessing its current cybersecurity capabilities, developing its national cybersecurity strategy and to establish its National Computer Incident Response Team (BS-CIRT). This will eventually serve as a trusted, central coordination point of contact for cybersecurity, aimed at identifying, defending against, responding to and managing cyber threats.

E. National cybersecurity strategy

Barbados does not have any officially recognised national cybersecurity strategy. In July 2019, the Barbados Government announced that it, with the support of the ITU, would formulate a new national ICT strategy over the following five years under five broad pillars utilising an ITU framework, namely rights, connectivity, government, economy, skills and inclusion.

F. Initiatives to combat cybercrime

- Barbados is a member of the Caribbean Community (CARICOM) and receives support from IMPACS in addressing cyberthreats and vulnerabilities. As a member state, Barbados also signed off on the CARICOM Cyber Security and Cybercrime Action Plan (CCSCAP) in 2017.
- Barbados is also one of the 195 INTERPOL [143] member countries.[144]

137 NCSI: Barbados, available at: https://ncsi.ega.ee/country/bb/ (accessed 17 January 2023).
138 Computer Misuse Act of 2005, available at: www.cavehill.uwi.edu/cits/information-security/resources-en/computer-misuse-act-2004.aspx (accessed 17 January 2023).
139 Telecommunications Act, available at: www.wipo.int/wipolex/en/text.jsp?file_id=209474 (accessed 17 January 2023).
140 Computer Misuse Act of 2005, section 5, available at: www.cavehill.uwi.edu/cits/information-security/resources-en/computer-misuse-act-2004.aspx (accessed 17 January 2023).
141 Ibid, section 13.
142 Ibid, section 6.
143 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
144 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).

- Barbados is working in partnership with ITU to assist the country in building and deploying the technical capabilities and related training necessary to develop its national cybersecurity strategy and to establish its CIRT. By extension, this project is expected to increase national cybersecurity capacity while moving forward on enhancing regional and international collaboration.

6. Belize

A. National cyber threat landscape

Belize recently promulgated cybercrime legislation. According to the National Cyber Security Index (NCSI),[145] as of January 2023 Belize ranked: 126th out of 161 countries on the NCSI with a score of 18.18; 159th out of 194 countries on the Global Cybersecurity Index; and 120th on the ICT Development Index.

B. National cybercrime legislation and related laws

- Cybercrime Act 2020[146]
- Telecommunication Act 2000[147]
- Interception of Communications Act 2010[148]
- Electronic Transactions Act 2003[149]

C. Scope/application of laws

- The Cybercrime Act was enacted to: combat cybercrime by creating cyber offences; provide for penalties, investigation and prosecution of the offences of cybercrime; and to provide for matters connected therewith or incidental thereto. It provides for cyber offences such as illegal access to a computer system, illegal access to computer data, illegal data interference, illegal system interference, illegal devices and codes, computer-related forgery, identity-related fraud, identity-related theft and child luring.
- The Telecommunication Act makes provision to ensure the security of telecommunication services. Part IV of the Act provides for cyber offences such as interception of computer data, illegal data or system interference, illegal access of computer data and fraudulent use of telecommunication systems.
- The Interception of Communications Act provides for the interception of communications and the provision of information relating to interception in Belize. Section 3 of the Act prohibits the interception of communication during its transmission by means of a public postal service or a communication network without authorisation. It also prohibits the interception of communications for commercial benefit, political advantage or criminal activity. The Act further prohibits other interception-related offences, such as encryption for the purpose of committing a crime, and prescribes sanction for its commission.[150]

---

145 NCSI: Belize, available at: https://ncsi.ega.ee/country/bz/ (accessed 17 January 2023).

146 Cybercrime Act, available at: www.nationalassembly.gov.bz/wp-content/uploads/2020/10/Act-No.-32-of-2020-Cybercrime.pdf (accessed 14 January 2023).

147 Telecommunications Act, sections 43–47, available at: //sherloc.unodc.org/cld/en/legislation/blz/telecommunications_act/part_iv/sections_43-47/sections_43-47.html (accessed 17 January 2023).

148 Interception of Communications Act, available at: https://sherloc.unodc.org/cld/v3/sherloc/legdb/search.html?lng=en#?c=%7B%22filters%22:%5B%7B%22fieldName%22:%22en%23__el.legislation.crimeTypes_s%22,%22value%22:%22Cybercrime%22%7D%5D,%22sortings%22:%22%22,%22match%22:%22belize%22,%22termMatch%22:%22belize%22%7D (accessed 13 January 2023).

149 Belize – Electronic Transactions Act 2003, available at: www.belizejudiciary.org/download/LAWS-of-Belize-rev2011/Laws-of-Belize-Update-2011/VOLUME%2011/Cap%20229.03%20Electronic%20Transactions%20Act.pdf

150 Interception of Communications Act, section 4, available at: https://sherloc.unodc.org/cld/v3/sherloc/legdb/search.html?lng=en#?c=%7B%22filters%22:%5B%7B%22fieldName%22:%22en%23__el.legislation.crimeTypes_s%22,%22value%22:%22Cybercrime%22%7D%5D,%22sortings%22:%22%22,%22match%22:%22belize%22,%22termMatch%22:%22belize%22%7D (accessed 13 January 2023).

- The Electronic Transactions Act 2003 was promulgated to: 'eliminate legal barriers to the effective use of electronic communications in transactions; promote the harmonisation of legal rules on electronic transactions across national boundaries; facilitate the appropriate use of electronic transactions; promote business and community confidence in electronic transactions; and enable business and the community to use electronic communications in their transactions with government.'

D. Sanctions/penalties for cyber-related crimes
A person who commits an offence under the Cybercrimes Act is liable on summary conviction to a fine between 3,000 and 10,000 dollars and a term of imprisonment between three and five years; and on conviction on indictment to a fine between 5,000 and 15,000 Belizean dollars and term of imprisonment between five to ten years. The court may further prohibit the offender from using the internet or any computer system.

E. National computer emergency response team (CERT)/computer security incident response team (CSIRT)
Belize does not yet have a national CERT/CIRT; however, there are ad hoc CERTs.

F. National cybersecurity strategy
The Belize National Cyber Security Strategy 2020–2030[151] was developed in collaboration with the government and stakeholders, to address cybersecurity threats and provide guidance on key actions to be taken to improve Belize's overall preparedness and responsiveness to these threats. This strategy outlines the principles and long-term goals that will form the basis and overall direction for the planning and development of the national cybersecurity position, including a plan of action outlining various roles and responsibilities for implementation.

G. Initiatives to combat cybercrime
- Belize is a member of the Caribbean Community (CARICOM) and receives support from IMPACS in addressing cyberthreats and vulnerabilities. As a member state, Belize also signed off on the CARICOM Cyber Security and Cybercrime Action Plan (CCSCAP).
- Belize is one of the 195 INTERPOL [152] member countries.[153]
- The Police Information Technology and Cyber Unit (PITCU) of the Belize Police Department (BPD) manages investigations of cyber-related crimes, as well as those felonies that involve electronic evidence. The PITCU has investigated cases of phishing, credit card and ATM fraud, as well as other crimes that involve electronic evidence, including drug trafficking. The PITCU has also reported that it has received reports of cyberbullying, revenge porn and identity theft. In terms of some international collaboration to counter cybercriminal activities, the PITCU works in partnership with the Internet Watch Foundation in order to report cases of child pornography.[154]
- Establishment of an Inter-institutional Cybersecurity Task Force with a vision to enhance Belize's cybersecurity position.
- Establishment of awareness programmes and attendance by relevant officials of trainings and workshops on combatting cybercrime; for example, Regional Conference on Cybercrime of the Budapest Convention by the Council of Europe for the Caribbean Community.[155]

151 National Cybersecurity Strategy – Towards A Secure Cyberspace 2020–2023, available at: www.pressoffice.gov.bz/wp-content/uploads/2019/12/belize-cybersecurity-strategy-2020-2023.pdf (accessed 20 February 2023).
152 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
153 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).
154 Belize Cybercrime Policies and Strategies, available at: www.coe.int/en/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/belize/pop_up?_101_INSTANCE_CmDb7M4RGb4Z_viewMode=print&_101_INSTANCE_CmDb7M4RGb4Z_languageId=en_GB (accessed14 March 2023).
155 Regional Conference on Cybercrime Strategies and Policies and features of the Budapest Convention for the Caribbean Community, available at: https://rm.coe.int/3148-1-1-3-final-report-dr-reg-conference-cy-policies-caribbean-comm-1/168098fb6c (accessed on 26 January 2023).

7. Botswana

A. National cyber threat landscape

According to the National Cyber Security Index (NCSI),[156] as of January 2023 Botswana ranked: 114th out of 161 countries on the NCSI with a score of 22.08; 88th out of 194 countries on the Global Cybersecurity Index; 105th on the ICT Development Index; and 102nd on the Networked Readiness Index.

B. National cybercrime legislation and related laws

- Cybercrime and Computer Related Crimes Act 2007[157]
- Electronic Communications and Transactions Act 2014[158]
- Electronic Communications and Transactions (Amendment) Act 2018[159]
- Communications Regulatory Authority Act 2012[160]
- Electronic Records (Evidence) Act 2014[161]
- Data Protection Act 2018[162]

C. Scope/application of laws

- The Cyber Crime and Computer Related Crimes Act 2007 was enacted to 'combat cybercrime and computer-related crimes, to repress criminal activities perpetrated through computer systems and to facilitate the collection of electronic evidence'. Part II of the Act provides for, and criminalises, cyber offences such as: unauthorised access to a computer or computer system,[163] unauthorised interference with a computer or computer system,[164] unlawful interception of data,[165] cyber extortion,[166] cyber fraud,[167] and electronic traffic in pornographic or obscene material.[168]
- The Electronic Communications and Transactions Act 2014 was enacted 'to provide for the facilitation and regulation of electronic communications and transactions; to provide specifically for electronic commerce and electronic signatures and for matters incidental and connected thereto'.
- The Communications Regulatory Authority Act 2012[169] provides for the regulation of the communications sector, comprising telecommunications, the internet, radio communications, broadcasting, postal services and related matters.

156 NCSI: Botswana, available at: https://ncsi.ega.ee/country/bw/ (accessed 14 January 2023).
157 Cybercrime and Computer Related Crimes Act, available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/Activities/SA/docs/SA-1_Legislations/Botswana/CYBERCRIMES.pdf (accessed 11 January 2023).
158 Electronic Communications and Transactions Act 2014, available at: www.bocra.org.bw/sites/default/files/Electronic-Communications-and-Transactions-Act-2014.pdf (accessed 11 January 2023).
159 Electronic Communications and Transactions Amendment Act 2018, available at: www.bocra.org.bw/electronic-communications-and-transactions-amendment-act-2018 (accessed 11 January 2023).
160 Botswana Communications Regulatory Authority, available at: www.bocra.org.bw/sites/default/files/documents/COMMUNICATIONS%20REGULATORY%20ACT%2C%202012.pdf (accessed 11 January 2023).
161 Electronic Records (Evidence), Principal Legislation, available at: https://botswanalaws.com/alphabetical-list-of-statutes/electronic-records-evidence (accessed 11 January 2023).
162 Data Protection Act, available at: www.cirt.org.bw/sites/default/files/2021-03/DataProtectionAct.pdf (accessed 11 January 2023).
163 Cybercrime and Computer Related Crimes Act, section 4, available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/Activities/SA/docs/SA-1_Legislations/Botswana/CYBERCRIMES.pdf (accessed 11 January 2023).
164 Ibid, section 8.
165 Ibid, section 9.
166 Ibid, section 14.
167 Ibid, section 15.
168 Ibid, section 16.
169 Botswana Communications Regulatory Authority, available at: www.bocra.org.bw/sites/default/files/documents/COMMUNICATIONS%20REGULATORY%20ACT%2C%202012.pdf (accessed 11 January 2023).

- The Electronic Records (Evidence) Act 2014[170] provides for the admissibility of electronic evidence in legal proceedings and authentication of electronic evidence.
- The Data Protection Act 2018 provides for the protection and safeguarding of personal data and other matters incidental to it.

D. Sanctions/penalties for cyber-related crimes
- The Cyber Crime and Computer Related Crimes Act 2007 provides liabilities for cyber offences to include fines ranging between 5,000 and 100 000 pula or imprisonment for a term ranging from three months to up to three years, or to both a fine and imprisonment.
- The Electronic Communications and Transactions Act 2014 in section 46 makes a general provision for offences and prescribes a penalty of a fine not exceeding 10,000 pula or to imprisonment for a term not exceeding five years, or to both a fine and imprisonment.

E. National computer emergency response team (CERT)/computer security incident response team (CSIRT)
The Computer Incident Response Team (CIRT) for Botswana (BwCIRT) provides an official point of contact for dealing with computer security incidents and emergency incident response at the national level for government departments, internet service providers (the telecommunications sector and internet community) and other relevant entities.[171] It also acts as 'the trusted point of contact', as well as providing central operational co-ordination for handling all types of information and computer security incidents.[172]

F. National cybersecurity strategy
The Botswana National Cybersecurity Strategy[173] comprises six core objectives: make Botswana more secure and resilient to cyberattacks; build cybersecurity capacity and capability in Botswana; raise and promote cybersecurity awareness among the general public; foster cybersecurity research and development; enhance collaboration and co-operation on cybersecurity issues at the national, regional and international levels; and to harness or leverage Botswana's cyberspace for socio-economic development.

H. Initiatives to combat cybercrime
- Botswana is one of the 195 INTERPOL [174] member countries.[175]
- Adoption of the Botswana National Information and Communications Technology Policy and e-commerce strategy (commonly called 'the Maitlamo').[176] The strategy, among other things, seeks to 'strengthen consumer protection, cybersecurity and fraud prevention measures, and foster the adoption of industry best practices in data security across e-commerce sites, payment gateways, system operators and service providers in the country'.[177]
- The recommendation to establish a Botswana multi-stakeholder National Cybersecurity Advisory Council (NCAC) to facilitate dedicated stakeholder engagements on cybersecurity and related matters in the country.

170 Electronic Records (Evidence), Principal Legislation, available at: https://botswanalaws.com/alphabetical-list-of-statutes/electronic-records-evidence (accessed 11 January 2023).
171 BwCirt, Home, available at: www.cirt.org.bw/ (accessed 11 January 2023).
172 Botswana National Cybersecurity Strategy, available at: www.cirt.org.bw/sites/default/files/2021-03/approved%20botswana-national-cybersecurity-strategy%20%281%29.pdf (accessed 11 January 2023).
173 Ibid.
174 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
175 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).
176 National Information and Communications Technology Policy, available at: https://unctad.org/system/files/official-document/dtlstict2021d4_en.pdf (accessed 26 January 2023).
177 Ibid.

- Establishment of the Botswana Digital Forensic Laboratory (DFL)[178] to allow for faster investigations and fact-finding by law enforcement.
- Botswana engages in international collaboration and co-ordination to combat cybercrimes. For instance, collaboration with the cybersecurity-executing arm of the International Telecommunication Union (ITU);[179] and the International Multilateral Partnership Against Cyber Threats (IMPACT).
- Alignment of Botswana's Cybercrime and Computer Related Crimes Act[180] with the South African Development Community (SADC) Model Law on Cybercrime[181] to combat evolving cyber threats.

8. Brunei Darussalam

A. National cyber threat landscape

According to the National Cyber Security Index (NCSI),[182] as of January 2023 Brunei Darussalam ranked: 82nd out of 161 countries on the NCSI with a score of 41.56; 85th out of 194 countries on the Global Cybersecurity Index; and 53rd on the ICT Development Index.

B. National cybercrime legislation and related laws
- Computer Misuse Act (Revised) 2007[183]
- Electronic Transactions Act No. 196 (revised in 2008)[184]

C. Scope/application of laws
- The Computer Misuse Act (CMA) makes provision for securing computer material against unauthorised access or modification and for matters related thereto. Part II of the Act provides for cyber offences such as: unauthorised access to computer material; access with intent to commit or facilitate commission of an offence; unauthorised modification of computer material; unauthorised use or interception of a computer service; unauthorised obstruction or use of a computer; and unauthorised disclosure of an access code.
- The Electronic Transactions Act makes provision for the security and use of electronic transactions and for connected purposes.

D. Sanctions/penalties for cyber-related crimes
- The CMA provides that anyone guilty of an offence under the Act shall be liable on conviction to a fine between $5,000 to $50, 000 Brunei Dollars or imprisonment for a term ranging between two years and ten years or both. Section 9 of the CMA provides for enhanced punishment for offences involving protected computers, of a fine not exceeding $100,000 Brunei Dollars or imprisonment for a term not exceeding 20 years or both. The Act further punishes abetments and attempts as offences.

E. National computer emergency response team (CERT)/computer security incident response team (CSIRT)

178 Digital Forensic Laboratory, available at: https://secur.co.bw/services/digital-forensics/ (accessed 13 January 2023).
179 ITU: Committed to Connecting the World (ITU), available at: www.itu.int:443/en/Pages/default.aspx (accessed 14 January 2023).
180 Cybercrime and Computer Related Crimes Act, available at: www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/Activities/SA/docs/SA-1_Legislations/Botswana/CYBERCRIMES.pdf (accessed 11 January 2023).
181 Computer Crime and Cybercrime: Southern African Development Community (SADC) Model Law, available at: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/SADC Model Law Cybercrime.pdf (accessed 13 March 2023).
182 NCSI: Brunei Darussalam, available at: https://ncsi.ega.bn/country/ag/ (accessed 17 January 2023).
183 Computer Misuse Act, available at: www.agc.gov.bn/AGC%20Images/LOB/pdf/Computer%20Misuse.pdf (accessed 18 January 2023).
184 Electronic Transactions Act , available at: www.agc.gov.bn/AGC%20Images/LOB/PDF/Electronic%20Transactions%20(chp.196).pdf (accessed 13 January 2023).

Brunei Computer Emergency Response Team (BruCERT)[185] was established in 2004 as the national CERT to deal with computer, internet and other related security threats and incidents in the country. It also collaborates with other regional and international CERTs to prevent and respond to security threats.[186]

F. National cybersecurity strategy

Brunei has what is referred to as the Brunei National Cyber Security Framework,[187] which is a set of voluntary standards, guidelines and processes that organisations can use to reduce the risk of cybersecurity threats. There is no record of a national cybersecurity strategy.

G. Initiatives to combat cybercrime

- Brunei is one of the 195 INTERPOL [188] member countries.[189]
- The government has recently intensified cybersecurity initiatives such as: implementation of the Regulations for Computer Abuse in June 2000, which later became the Computer Misuse Act;[190] adoption of the Child Online Protection Framework;[191] and issuance of ICT Risk Management Guidelines to local banks and finance companies.[192]
- Development of a national cybersecurity framework to establish the security standards necessary for cyber risk management and compliance.[193]
- International collaboration and co-ordination to combat cybercrime. For instance, BruCERT[194] is a member of international security expert organisations such as the Asia Pacific CERT (APCERT), the Organization of the Islamic Cooperation – Computer Emergency Response Teams (OIC-CERT) and the Forum of Incident Response and Security Teams (FIRST) for dealing with IT security-related incidents and co-ordinating with other CERTs in fighting cybercrime worldwide.
- Establishment of IT Protective Security Services (ITPSS), which consists of information security and cybersecurity experts. ITPSS is a Brunei Darussalam referral agency for dealing with internet threats and computer security problems.[195]
- Establishment of Cyber Security Brunei (CSB), which is the national cybersecurity agency serving as an administrator that monitors and co-ordinates national efforts in addressing cybersecurity threats and cybercrime. It operates under the Ministry of Transport and Infocommunications (MTIC), with the Minister of MTIC as Minister-in-charge of Cybersecurity.
- Facilitation of public awareness on cybersecurity and cyber safety through outreach projects and seminars such as the Vigilance Program for Internet Ethics and Cyber Security.[196]

185 Brunei Computer Emergency Response Team, available at: www.csb.gov.bn/brucert (accessed 27 January 2023).
186 Ibid.
187 Cyber Security Brunei – National Cyber Security Framework, available at: https://csb.gov.bn/brunei-national-cyber-security-framework (accessed 27 February 2023).
188 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
189 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).
190 Computer Misuse Act, available at: www.agc.gov.bn/AGC%20Images/LOB/pdf/Computer%20Misuse.pdf (accessed 18 January 2023).
191 Sharbawi, Z (2011), The 11th China-ASEAN Prosecutors-General Conference, Attorney General Chamber of Brunei Darussalam, available at: www.agc.gov.bn/conference/Secretariat%20Documents/Speech%20and%20Key%20Notes/Brunei%20Key%20Note%20Sp (accessed 25 January 2023).
192 Gan, RY (2018), Brunei Cyberspace Masterplan 2018, ResearchGate, 4.
193 Sharbawi, Z (2011), The 11th China-ASEAN Prosecutors-General Conference, Attorney General Chamber of Brunei Darussalam, available at: www.agc.gov.bn/conference/Secretariat%20Documents/Speech%20and%20Key%20Notes/Brunei%20Key%20Note%20Sp (accessed 25 January 2023).
194 Brunei Computer Emergency Response Team, available at: www.csb.gov.bn/brucert (accessed 27 January 2023).
195 Bhirowo, M (2018), 'Brunei Darussalam's E-Government Strategy in Overcoming Cyber Threats', *Jurnal Pertahanan* 4(3), 146.
196 Brunei Darussalam's E-Government Strategy in Overcoming Cyber Threats, available at: www.researchgate.net/publication/330664232_BRUNEI_DARUSSALAMS_E-GOVERNMENT_STRATEGY_IN_OVERCOMING_CYBER_THREATS (accessed 28 January 2023).

9. Cameroon

A. National cyber threat landscape

As has been the case in most African countries, the cyber threat landscape in Cameroon has witnessed a huge growth in incidents. In 2014, it was reported that 'cyber criminality cost 3.5 billion to Cameroon between November and December 2013'.[197] According to the National Cyber Security Index (NCSI),[198] as of January 2023 Cameroon ranked: 96th on the NCSI with a score of 32.47; 93rd on the Global Cybersecurity Index; 149th on the ICT Development Index; and 114th on the Networked Readiness Index.

B. National cybercrime legislation and related laws

- Law No. 2010/012 of 21 December 2010 Relating to Cybersecurity and Cybercriminality in Cameroon[199]
- Law No. 2010/013 of 21 December 2010 Governing Electronic Communications in Cameroon[200]
- Law No. 2010/013 (Amendment Law of April 2015)[201]
- Law No. 2010/021 of 21 December 2010 Governing Electronic Commerce in Cameroon[202]
- Law No. 2016/007 of 12 July 2016 Relating to the Penal Code[203]
- Regulation No. 01/CEMAC/UMAC/CM of 4th April 2003[204]
- Law No. 2005/007 of 27 July 2005 Establishing the Criminal Procedure Code[205]
- Decree No. 2012/180 of 10 April 2012 on the Establishment, Organisation and Functioning of the National Agency of Information and Communication Technology[206]

C. Scope/application of laws

- Law No. 2010/012 of 21 December 2010 ('Cyberlaw')[207] is the main legislation on cybercrime and cybersecurity in the country. It governs the security framework of electronic communication networks and information systems, and defines and punishes offences related to the use of information and communication technologies in Cameroon.

---

197 Rene, NN (2021), the Legal and Institutional Framework for the Enforcement of Cybersecurity Regulations in Cameroon, 15 February, available at: https://papers.ssrn.com/abstract=3835221 (accessed 12 January 2023).

198 NCSI: Cameroon, available at: https://ncsi.ega.ee/country/cm/ (accessed 14 January 2023).

199 Law No. 2010/012 of 21 December 2010 Relating to Cybersecurity and Cybercriminality in Cameroon, available at: https://ictpolicyafrica.org/api/documents/download?_id=5ebc1455becbe0001b2536c3 (accessed 12 January 2023).

200 Law No. 2010/013 of 21 December 2010 Governing Electronic Communications in Cameroon, available at: www.minpostel.gov.cm/index.php/en/les-textes/postes/lois/180-law-no-2010-013-of-21-december-2010-governing-electronic-communications-in-cameroon (accessed 14 January 2023).

201 Law No. 2010/013 (Amendment Law of April 2015), available at: http://www.art.cm/sites/default/files/documents/LOI_2015_06_modifiant_2010_13_du_21_10_2010_communications_electroniques.pdf (accessed 14 January 2023).

202 Laws and Regulation (CamGovCA), available at: https://camgovca.cm/en/regulation-policy/laws-and-regulations.html (accessed 14 January 2023).

203 Law No. 2016/007 of 12 July 2016 Relating to the Penal Code, available at: www.prc.cm/en/news/the-acts/laws/1829-law-no-2016-007-of-12-july-2016-relating-to-the-penal-code (accessed 12 January 2023).

204 Regulation No. 01/CEMAC/UMAC/CM of 4 April 2003 on the Prevention and Suppression of Money Laundering and Financing Terrorism in Central Africa, available at: www.anif.cm/images/pdfanif/CEMAC_Regulation.pdf (accessed 12 January 2023).

205 Law No. 2005/007 of 27 July 2005 on the Criminal Procedure Code, available at: www.minjustice.gov.cm/index.php/en/instruments-and-laws/laws/290-law-no-2005-007-of-27-july-2005-on-the-criminal-procedure-code (accessed 14 January 2023).

206 Decree No. 2012/180 of 10 April 2012, available at: https://camgovca.cm/en/regulation-policy/laws-and-regulations.html#decree-no-2012-180-of-10-april-2012-on-the-establishment-organization-and-functioning-of-national-agency-of-information-and-communication-technology (accessed 14 January 2023).

207 Law No. 2010/012 of 21 December 2010 Relating to Cybersecurity and Cybercriminality in Cameroon, available at: https://ictpolicyafrica.org/api/documents/download?_id=5ebc1455becbe0001b2536c3 (accessed 12 January 2023).

- Law No. 2010/021 of 21 December 2010[208] generally governs electronic commerce in Cameroon. It further provides for principles governing the exercise of electronic commerce-related activities, and the offences and penalties related to them.
- Law No. 2005/007 of 27 July 2005 establishing the Criminal Procedure Code[209] and Law No. 2016/007 of 12 July 2016 relating to the Penal Code[210] provide a framework for procedural measures in criminal matters.

D. Sanctions/penalties for cyber-related crimes

- Chapter II of the Cyberlaw provides for offences and their penalties. Some of the offences include: unauthorised access to an electronic communication network or an information system or a terminal device;[211] disturbance or disruption of the functioning of an electronic communication network;[212] fraudulently accessing an electronic communication network or an information system;[213] recording or publishing without consent and for financial gain, images that undermine the bodily integrity of another person through electronic communications or an information system;[214] and child pornography.[215] Penalties include imprisonment from two to ten years or a fine from 1,000,000 to 50,000,000 CFA francs or both such fine and imprisonment.
- Law No. 2010/021 of 21 December 2010 governing electronic commerce in Cameroon[216] provides for offences and penalties in part V of the law. The offences include: the illegal use of electronic signature of another,[217] and forcing another to subscribe to an electronic sale.[218] The penalty for illegal use of electronic signature of another is as prescribed by section 219 of the Penal Code,[219] which provides the punishment of imprisonment from one month to one year or a fine of 100,000 to 1,000,000 CFA francs or with both such imprisonment and fine.

E. National computer emergency response team (CERT)/computer security incident response team (CSIRT)

Cameroon's Computer Incident Response Team[220] is the country's centre for alerts and responses to computer attacks. It facilitates the identification of threats to the national cyber-space and collaborates with similar organisations in other countries to create a secure national digital space for the country.

208 Laws and Regulation (CamGovCA), available at: https://camgovca.cm/en/regulation-policy/laws-and-regulations.html (accessed 14 January 2023).
209 Law No. 2005/007 of 27 July 2005 on the Criminal Procedure Code, available at: http://www.minjustice.gov.cm/index.php/en/instruments-and-laws/laws/290-law-no-2005-007-of-27-july-2005-on-the-criminal-procedure-code (accessed 14 January 2023).
210 Law No. 2016/007 of 12 July 2016 Relating to the Penal Code, available at: www.prc.cm/en/news/the-acts/laws/1829-law-no-2016-007-of-12-july-2016-relating-to-the-penal-code (accessed 12 January 2023).
211 Law No. 2010/012 of 21 December 2010 Relating to Cybersecurity and Cybercriminality in Cameroon, section 65, available at: https://ictpolicyafrica.org/api/documents/download?_id=5ebc1455becbe0001b2536c3 (accessed 12 January 2023).
212 Ibid, section 66.
213 Ibid, section 68.
214 Ibid, section 75.
215 Ibid, section 76.
216 Laws and Regulation (CamGovCA), available at: https://camgovca.cm/en/regulation-policy/laws-and-regulations.html (accessed 14 January 2023).
217 Law No. 2010/021 of 21 December 2010 Governing Electronic Commerce in Cameroon, section 42, available at: https://camgovca.cm/en/regulation-policy/laws-and-regulations.html (accessed 14 January 2023).
218 Ibid, section 44.
219 Law No. 2016/007 of 12 July 2016 Relating to the Penal Code, available at: www.prc.cm/en/news/the-acts/laws/1829-law-no-2016-007-of-12-july-2016-relating-to-the-penal-code (accessed 12 January 2023).
220 Cameroon Computer Incident Response Team, available at: www.cirt.cm/ (accessed 14 January 2023).

F. National cybersecurity strategy

As at the time of this research, Cameroon did not seem to have adopted a cybersecurity strategy. What is in place is the Strategic Plan for a Digital Cameroon,[221] launched by the government in May 2016.

G. Initiatives to combat cybercrime

- Cameroon is one of the 195 INTERPOL [222] member countries.[223]
- Creation of the National Cyber Expertise Centre[224] to prevent cybercrimes.
- Creation of the National Agency for Information and Communication Technologies (ANTIC).[225]
- Creation of the Telecommunications Regulatory Board (TRB).[226]
- Launch of the Strategic Plan for a Digital Cameroon,[227] which highlights actions to be carried out and appropriate measures to develop ICT uses for the emergence of a safe and secure digital economy in Cameroon.[228]
- Creation of the Special Unit for the Fight against Cybercrime within the Judicial Police Directorate, to ensure cybercrimes are dealt with thoroughly and expeditiously.

10. Canada

A. National cyber threat landscape

According to the National Cyber Security Index (NCSI),[229] as of January 2023 Canada ranked: 31st out of 161 countries on the NCSI with a score of 70.13; 8th out of 194 countries on the Global Cybersecurity Index; 29th on the ICT Development Index; and 11th on the Networked Readiness Index. Canada has experienced a marked increase in the rate of cybercrime in recent years. Between 2017 and 2021, it was reported that 'cybercrime increased by 153%, from 27,829 cases in 2017 to 70,288 cases in 2021'.[230]

B. National cybercrime legislation and related laws

- Criminal Code of 1985[231]
- Communications Security Establishment Act (CSE Act)[232]
- Canadian Anti-Spam Legislation (CASL)[233]

---

221 Available at: https://cyrilla.org/en/entity/sz9xamosxns?page=1 (accessed 14 January 2023).
222 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
223 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).
224 *Cameroon Tribune* (2015), 'Cyber-Crime Fighting Centre Opens in Buea', 22 July, available at: http://ct2015.cameroon-tribune.cm/index.php?option=com_content&view=article&id=91124:cyber-crime-fighting-centre-opens-in-buea&catid=4:societe&Itemid=3> (accessed 12 January 2023).
225 National Agency for Information and Communication Technologies, available at: www.antic.cm/index.php/en> (accessed 12 January 2023).
226 Telecommunications Regulatory Board of Cameroon, available at: http://www.art.cm/site/index.php/en/ (accessed 12 January 2023).
227 Available at: https://cyrilla.org/en/entity/sz9xamosxns?page=1 (accessed 14 January 2023).
228 Ibid.
229 NCSI: Canada, available at: https://ncsi.ega.ee/country/ca/ (accessed 17 January 2023).
230 'The Latest 2023 Cyber Crime Statistics', available at: https://aag-it.com/the-latest-cyber-crime-statistics/ (accessed 9 January 2023).
231 Criminal Code, available at: https://laws-lois.justice.gc.ca/PDF/C-46.pdf (accessed 14 January 2023).
232 Consolidated Federal Laws of Canada, Communications Security Establishment Act (1 August 2019), available at: https://laws-lois.justice.gc.ca/eng/acts/C-35.3/page-1.html (accessed 23 January 2023).
233 Canadas Anti-Spam Legislation, Home, 19 March 2021, available at: https://fightspam-combattrelepourriel.ised-isde.canada.ca/site/canada-anti-spam-legislation/en/canadas-anti-spam-legislation (accessed 23 January 2023).

- Copyright Act[234]
- Evidence Act 2010[235]

C. Scope/application of laws

- The Criminal Code is the substantive criminal law in Canada. It provides for offences such as publication of an intimate image without consent, child pornography, identity fraud, forgery, interception of communications,[236] unauthorised use of a computer,[237] and possession of a device to obtain unauthorised use of a computer system or to commit mischief.[238]
- CASL protects consumers and businesses from the misuse of digital technology, including spam and other electronic/cyber threats. It prohibits actions such as the alteration or transmission of data in an electronic message.
- The CSE Act establishes the Communications Security Establishment, whose mandate includes ensuring cybersecurity and information assurance, foreign intelligence, and defensive and active cyber operations in Canada.

D. Sanctions/penalties

- The Criminal Code prescribes liability for offenders of cyber or cyber-related crimes to range from imprisonment for two to fourteen years. However, if threat to human life is involved or the activity impacts human life, such offender can be liable to life imprisonment.
- The CASL prescribes an administrative penalty of up to 1 million Canadian dollars for individuals, and 10 million Canadian dollars (C$) for others.
- The Copyright Act provides remedy of 'a fine of not more than $1,000,000 or to imprisonment for a term of not more than five years or to both', for conviction on indictment; and 'a fine of not more than $25,000 or to imprisonment for a term of not more than six months or to both' for summary conviction.[239]

E. National computer emergency response team (CERT)/computer security incident response team (CSIRT)

The Canadian Cyber Incident Response Center (CCIRC)[240] is the entity entrusted with co-ordinating computer incident emergency response.

F. National cybersecurity strategy

The current national cyber security strategy[241] is based on the Cyber Security Action Plan (2019–2024).[242] The strategy stipulates Canada's vision for security and prosperity in the digital age. It has been reported that 'cybercrime in Canada causes more than $3 billion in economic losses each year'.[243] In 2010, the government launched Canada's first cybersecurity strategy. As a means to address the evolving cyber threat landscape, a cyber review was conducted in the country in 2016, with wide public consultation. The review paved the way for an improved

234 Consolidated Federal Laws of Canada, Copyright Act (30 December 2022), available at: https://laws.justice.gc.ca/eng/acts/C-42/index.html (accessed 23 January 2023).
235 Evidence Act, available at: https://laws-lois.justice.gc.ca/PDF/C-5.pdf (accessed 13 January 2023).
236 Article 184, Criminal Code, available at: https://laws-lois.justice.gc.ca/PDF/C-46.pdf (accessed 14 January 2023).
237 Ibid, Article 342.1.
238 Ibid, Article 342.2.
239 Consolidated Federal Laws of Canada, Copyright Act (30 December 2022), section 42, available at: https://laws.justice.gc.ca/eng/acts/C-42/index.html (accessed 23 January 2023).
240 The Canadian Cyber Incident Response Center (CCIRC) (2018), 'Collection of Digital Information', 21 December, available at: www.publicsafety.gc.ca/cnt/trnsprnc/ccss-nfrmtn-prvc/prvc-mpct-ssssmnt/cndn-cbr-ncdnt-en.aspx (accessed 23 January 2023).
241 National Cyber Security Strategy, available at: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx (accessed 13 March 2023).
242 Public SafetyCanada (2019), National Cyber Security Action Plan (2019–2024), 7 August, available at: www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019/index-en.aspx (accessed 23 January 2023).
243 Ibid.

national cybersecurity strategy, which was released in 2018. The strategy has three primary goals: to create secure and resilient Canadian systems; to create an innovative and adaptive cyber ecosystem; and to provide effective leadership, governance and collaboration.[244]

G. Initiatives to combat cybercrime

- Canada is a signatory to the Convention on Cybercrime (ETS No. 185)[245] of 23rd November 2001. It ratified the convention on 8 July 2015, while it came into force in the country on 1 November 2015.[246]
- Canada acceded to the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224)[247] on 12 May 2022. The protocol 'provides tools for enhanced co-operation and disclosure of electronic evidence – such as direct co-operation with service providers and registrars, effective means to obtain subscriber information and traffic data, immediate co-operation in emergencies or joint investigations – that are subject to a system of human rights and rule of law, including data protection safeguards'.[248]
- Canada is one of the 195 INTERPOL [249] member countries.[250]
- To combat cybercrime in the country, the government provides sufficient funding for cybersecurity. For instance, the government allocated close to C$1 billion on the 2018 and 2019 federal budgets.[251] The 2019 budget also included C$145 million to protect Canada's critical cyber systems, and another C$80 million over four years to support three or more Canadian cybersecurity networks across Canada.[252]
- Creation of a National Cybersecurity Action Plan (2019–2024).[253] The action plan lays out the specific cybersecurity initiatives planned by the government, and the ways and strategies to bring the plan to action.
- Establishment of innovative centres designed to combat cybercrime. These include creation of the Canadian Center for Cybersecurity[254] as the technical authority on cybersecurity to prepare for, respond to, mitigate and help recovery from cyber incidents; creation of Canada's Communications Security Establishment;[255] and the Cyber Security Cooperation Program (CSCP).[256]
- Implementation of public safety guidance on the fundamentals of cybersecurity for Canada's critical infrastructural community.[257]

---

244 Ibid.
245 Council of Europe, 'The Budapest Convention (ETS No. 185) and its Protocols', available at: www.coe.int/en/web/cybercrime/the-budapest-convention (accessed 26 January 2023).
246 Council of Europe, 'Complete list of Council of Europe's treaties', Treaty Office, available at: www.coe.int/en/web/conventions/full-list (accessed 25 January 2023).
247 Council of Europe, 'Enhanced co-operation and disclosure of electronic evidence: 22 Countries Open the Way by Signing the Second Additional Protocol to the Cybercrime Convention', available at: www.coe.int/en/web/cybercrime/second-additional-protocol/-/asset_publisher/isHU0Xq21Ihu/content/opening-coecyber2ap (accessed 26 January 2023).
248 Ibid.
249 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
250 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).
251 Ibid.
252 Ibid.
253 National Cyber Security Action Plan (2019–2024) (7 August 2019), available at: www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2019/index-en.aspx (accessed 25 January 2023).
254 Canadian Centre for Cyber Security, 28 October 2022, available at: https://cyber.gc.ca/en (accessed 23 January 2023).
255 Communications Security Establishment, 6 May 2020, available at: www.cse-cst.gc.ca/en (accessed 23 January 2023).
256 Cyber Security Cooperation Program, 21 December 2018, available at: www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/cprtn-prgrm/index-en.aspx (accessed 23 January 2023).
257 Fundamentals of Cyber Security for Canadas CI Community, 21 December 2018, available at: www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-fndmntls-cybr-scrty-cmmnty/index-en.aspx (accessed 23 January 2023).

- Enactments of legislation, such as Bill C-26[258] to amend the Telecommunications Act[259] and implement cybersecurity protections for telecom service providers.
- Introduction of initiatives in the Royal Canadian Mounted Police (RCMP), which 'analyses criminal intelligence from a wide array of sources, identifies emerging cybercrime threats, and makes links between cybercrime and other criminal domains, such as organised crime or financial crime'.[260] There is also the RCMP National Child Exploitation Coordination Centre (NCECC), which collaborates with other government and non-government agencies locally and internationally to combat the online sexual exploitation of children. Further, the NCECC also collaborates with the Canadian Centre for Child Protection in preventing the online sexual exploitation of children.[261]
- Canada also has the Canadian Anti-Fraud Centre (CAFC),[262] where online mass marketing fraud can be reported and mitigated.

11. Cyprus

A. National cyber threat landscape

According to the National Cyber Security Index (NCSI),[263] as of January 2023 Cyprus ranked: 38th out of 161 countries on the NCSI with a score of 66.23; 41st out of 194 countries on the Global Cybersecurity Index; 89th on the ICT Development Index; and 38th on the Networked Readiness Index.

B. National cybercrime legislation and related laws

- The Cyprus Law No. 22 (III) – 2004 ratifying the Convention on Cybercrime[264]
- Law 147(I)/2015 – implements Directive 2013/40/EU on Attacks Against Information Systems
- Law on the Legal Framework for Electronic Signatures and Associated Matters of 2004, Law No. 188(I)/2004[265]
- Cyprus Law L 91(I)/2014 – ratifies the EU Directive 2011/93/EE
- The Law on the Processing of Personal Data, L.138(I)/2001

C. Scope/application of laws

- Cyprus Law No. 22 (III) ratifies the Budapest Convention on Cybercrime and provides for cybercrimes such as hacking, child pornography, internet fraud and fraud from electronic communications.
- Law L 91(I)/2014 ratifies the EU Directive 2011/93/EE. It revises the legal framework on the prevention and combatting of sexual abuse, sexual exploitation of children and child pornography.[266]

258 Government of Canada Department of Justice, Bill C-26: An Act to Amend the Parliament of Canada Act and to Make Consequential and Related Amendments to Other Acts, 14 December 2022, available at: www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c26_1.html (accessed 23 January 2023).

259 Consolidated Federal Laws of Canada, Telecommunications Act (29 June 2021), available at: https://laws-lois.justice.gc.ca/eng/acts/t-3.4/ (accessed 23 January 2023).

260 Government of Canada, Royal Canadian Mounted Police (RCMP) Cybercrime Strategy, Royal Canadian Mounted Police, 2 December 2015, available at: www.rcmp-grc.gc.ca/en/royal-canadian-mounted-police-cybercrime-strategy (accessed 25 January 2023).

261 Ibid.

262 Government of Canada, RCMP, Canadian Anti-Fraud Centre, 27 December 2019, available at: https://antifraudcentre-centreantifraude.ca/index-eng.htm (accessed 31 January 2023).

263 NCSI: Cyprus, available at: https://ncsi.ega.ee/country/cy/ (accessed 17 January 2023).

264 Cyprus Law No. 22 (III), available at: www.ilo.org/dyn/natlex/docs/ELECTRONIC/100675/120828/F747771519/CYP100675%20Grk.pdf (accessed 14 January 2023).

265 Law on the Legal Framework for Electronic Signatures and Associated Matters of 2004, available at: https://sas-space.sas.ac.uk/5503/1/1756-2377-1-SM.pdf (accessed 14 January 2023).

266 Cyprus Police, available at: http://www.police.cy/police/police.nsf/index_en/index_en?opendocument (accessed 18 January 2023).

D. National computer emergency response team (CERT)/computer security incident response team (CSIRT)
Cyprus National Computer Security Incident Response Team (National CSIRT–CY)[267] is entrusted with the national responsibility of computer incident emergency response.

E. National cybersecurity strategy
The National Cybersecurity Strategy of Cyprus[268] reviewed the previous 2013 cybersecurity strategy of the country and aims to 'establish a safe electronic environment in the Republic of Cyprus, with specific considerations and actions for the protection of critical information infra-structures, whose disruption or destruction would have severe consequences to vital societal functions'.[269]

F. Initiatives to combat cybercrime
- Cyprus is a signatory to the Convention on Cybercrime (ETS No. 185)[270]. It ratified the convention on 19 January 2005, with it coming into force in the country on 1 May 2005.[271]
- Cyprus is one of the 195 INTERPOL [272] member countries.[273]
- Establishment of the Office for Combating Cybercrime (OCC)[274] for Cyprus Police.[275] The OCC specialises in the investigation of cybercrime, having been established in September 2007 based on Police Order No. 3/45 in order to implement the Law on the Convention on Cybercrime (Ratifying Law) L.22(III)/2004.[276] It therefore has the power and responsibility to investigate computer and internet-related crimes, and such related offences laid down by the law.
- Establishment of the Digital Evidence Forensic Laboratory (DEFL) in 2009, to ensure proper examination of electronic data and evidence. The laboratory is staffed with personnel trained in the collection and forensic analysis of electronic devices. They also serve as expert witnesses and give evidence in court when required.
- Implementation in January 2014 of the Cybercrime Reporting Platform to ensure prompt and easy reporting of cyber incidents in the country.
- International collaboration and co-operation through bilateral and multilateral agreements in exchanging information on threats and challenges in cyberspace. For instance, the OCC co-operates and collaborates with Europol, the European Union Cybercrime Taskforce (EUCTF), the European Network and Information Security Agency (ENISA), the International Criminal Police Organization (INTERPOL) and a number of other agencies.
- Establishment of the Cyprus Cybercrime Centre of Excellence (3CE).[277]

---

267 National Computer Security Incident Response Team of Cyprus, available at: https://csirt.cy/ (accessed 27 January 2023).
268 Cybersecurity Strategy, available at: www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CybersecurityStrategyoftheRepublicofCyprusv10_English.pdf (accessed 25 January 2023).
269 Ibid.
270 Council of Europe, 'The Budapest Convention (ETS No. 185) and its Protocols', available at: www.coe.int/en/web/cybercrime/the-budapest-convention (accessed 26 January 2023).
271 Council of Europe, 'Complete list of Council of Europe's treaties', Treaty Office, available at: www.coe.int/en/web/conventions/full-list (accessed 25 January 2023).
272 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
273 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).
274 Office for Combating Cybercrime of Cyprus Police, available at: www.police.gov.cy/police/police.nsf/All/671EB91BDCAA303EC22584000041D696?OpenDocument#:~:text=The%20specialised%20body%20for%20cybercrime,22(III)%2F2004 (accessed 27 January 2023).
275 Cyprus Police, available at: http://www.police.cy/police/police.nsf/index_en/index_en?opendocument (accessed 25 January 2023).
276 Cyprus Law No. 22 (III), available at: www.ilo.org/dyn/natlex/docs/ELECTRONIC/100675/120828/F747771519/CYP100675%20Grk.pdf (accessed 14 January 2023).
277 Council of Europe, 'Octopus Cybercrime Community', Asset Publisher, available at: www.coe.int/en/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/bahamas/pop_up (accessed 25 January 2023).

h. Publication of the new Cybersecurity Strategy[278] by the Ministry of Research, Innovation and Digital Policy. The strategy embodies various actions to combat cyber threats: creation of an integrated legislative and regulatory framework; creation and/or adaptation of the necessary structures and mechanisms; formulation of appropriate technical and organisational measures; development of the necessary skills and appropriate training; effective co-operation between the state and the competent bodies of the public/private sectors; and development of research and innovation.[279]

12. Dominica

A. National cyber threat landscape
According to the National Cyber Security Index (NCSI),[280] as of January 2023 Dominica ranked: 158th out of 161 countries on the NCSI with a score of 3.90; 174th out of 194 countries on the Global Cybersecurity Index; and 77th on the ICT Development Index.

B. National cybercrime legislation and related laws
- Computer and Computer Related Crime Act 2005[281]
- Electronic Funds Transfer Act No. 17 of 2013[282]
- Electronic Transactions Act, Act 19/2013[283]

C. Scope/application of laws
- The Computer and Computer Related Crime Act provides for such crimes as illegal access to a computer system to commit an offence, illegal interference with the functioning of a computer system, interception of data, and child pornography.
- The Electronic Funds Transfer Act provides for cyber offences such as forgery and electronic fraud.
- The Electronic Transactions Act gives legal effect to electronic documents, records and signatures and other related matters.

D. National computer emergency response team (CERT)/computer security incident response team (CSIRT)
Dominica does not currently have an officially recognised CERT/CSIRT.

E. National cybersecurity strategy
The Government of Dominica does not have a designated national cybersecurity strategy.

F. Initiatives to combat cybercrime
- Dominica is a member of the Caribbean Community (CARICOM)[284] and receives support from IMPACS in addressing cyberthreats and vulnerabilities. As a member state, Dominica also signed off on the CARICOM Cyber Security and Cybercrime Action Plan (CCSCAP).
- Dominica is one of the 195 INTERPOL [285] member countries.[286]

278 Cybersecurity Strategy, available at: www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/CybersecurityStrategyoftheRepublicofCyprusv10_English.pdf (accessed 25 January 2023).
279 Ibid.
280 NCSI: Dominica, available at: https://ncsi.ega.ee/country/dm/ (accessed 17 January 2023).
281 Computer and Computer Related Crime Act, available at: //sherloc.unodc.org/cld/en/legislation/dma/computer_and_computer_related_crime_act/part_ii_offences/article_5_-_10/computer_and_computer_related_crime_act.html (accessed 18 January 2023).
282 Database of Legislation, available at: //sherloc.unodc.org/cld/en/v3/sherloc/legdb/search.html (accessed 18 January 2023).
283 Electronic Transactions Act, available at: http://www.dominica.gov.dm/laws/2013/Electronic%20Transactions%20Act,%202013%20Act%2019%20of%202013.pdf (accessed 18 January 2023).
284 PublicTechnology.net (2022), 'No one is an island: how Caribbean states are working together to tackle cybercrime, 17 October, available at: https://publictechnology.net/articles/features/no-one-island-how-caribbean-states-are-working-together-tackle-cybercrime (accessed 24 January 2023).
285 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
286 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).

c. Dominica has continued to develop and implement international co-operation and facilitation of workshops: for instance, the Cyber Crime National Needs Assessment Workshop. Another was the workshop jointly facilitated by experts from the Organization of American States (OAS) through its Cyber Crime Unit, the Inter-American Committee against Terrorism (CICTE) and the Commonwealth Telecommunications Organisation (CTO), all of which have pledged support to Dominica in its endeavours.[287]

13. Eswatini

A. National cyber threat landscape

Eswatini passed cybercrime legislation in 2022. There is no cyber threat landscape assessment rating for Eswatini on the National Cyber Security Index (NCSI).[288]

B. National cybercrime legislation and related laws

- Computer Crime and Cyber Crime Act 2022[289]
- Electronic Communications and Transaction Act 2022[290]
- Data Protection Act 2022[291]

C. Scope/application of laws

- The Computer Crime and Cyber Crime Act 2022[292] criminalises offences committed against, and through the usage of, computer systems and electronic communications networks; provides for investigation and collection of evidence for computer and network-related crimes; provides for the admission of electronic evidence for such offences; establishes the National Cybersecurity Advisory Council; and gives powers to the Eswatini Communications Commission to regulate and co-ordinate cybersecurity matters and to provide for incidental matters.

  Part II of the Act prescribes for computer offences such as illegal access, illegal interception, illegal data interface, data espionage, illegal system interference, computer-related forgery and uttering, computer-related fraud, phishing, cyber terrorism, child pornography, identity-related crimes, cyber bullying and cyber stalking, website defacement, racist and xenophobic activities, genocide and harassment utilising means of electronic communication.

- The Electronic Communications and Transaction Act regulates electronic transactions, electronic communications, and the use of e-government services and other incidental matters.
- The Data Protection Act provides for the collection, processing, disclosure and protection of personal data, as well as balancing competing values of personal information privacy and sector-specific laws and other related matters.

D. Sanctions/penalties for cyber-related crimes

- Part II of the Computer Crime and Cyber Crime Act prescribes sanctions for offences committed. An offender may be liable on conviction to a fine between 100,000 to 1 million emalangeni or to imprisonment not exceeding 3 to 20 years, or both.

---

287 GIS Dominica, 'Dominica works to improve cyber crime resilience with support of international partners', available at: http://news.gov.dm/news/1647-dominica-works-to-improve-cyber-crime-resilience-with-support-of-international-partners (accessed 25 January 2023).

288 NCSI: Ranking (ega.ee), available at: https://ncsi.ega.ee/ncsi-index/ (accessed 3 March 2023).

289 Computer Crime and Cyber Crime 2020 Act, available at: www.esccom.org.sz/legislation/COMPUTER%20CRIME%20&%20CYBERCRIME%20ACT.pdf (accessed 13 January 2023).

290 Electronic Communications and Transaction Act, available at: www.gov.sz/images/ICT/ELECTRONIC-COMMUNICATIOACT.pdf (accessed 13 January 2023).

291 Data Protection Act, available at: www.gov.sz/images/ICT/DATA-PROTECTION-ACT.pdf (accessed 13 January 2023).

292 Computer Crime and Cyber Crime 2020 Act, available at: www.esccom.org.sz/legislation/COMPUTER%20CRIME%20&%20CYBERCRIME%20ACT.pdf (accessed 13 January 2023).

- Section 45(2) of the Electronic Communications and Transaction Act prescribes liability for 'a person, company, partnership, firm, business, society or association of persons convicted of an offence under this section to a fine not exceeding one hundred thousand emalangeni (E100,000) or imprisonment of a period not exceeding five years or both'.

E. National computer emergency response team (CERT)/computer security incident response team (CSIRT)
Eswatini Computer Incident Response Team (SzCIRT) acts as a focal point in co-ordinating cybersecurity incidents for government departments, internet service providers and other relevant entities within the country. It monitors incidents, provides early warnings, disseminates information, and enforces cybersecurity standards and minimum specifications for Eswatini.[293]

F. National cybersecurity strategy
The Eswatini National Cybersecurity Strategy[294] (NCS) 2020–2025 contains five strategic goals: enhance the security and resilience of national critical information infrastructure and other related ICT systems; strengthen the cybersecurity governance, policy, regulatory and legislative frameworks of Eswatini; build Eswatini's capacity and expertise in cybersecurity; foster a safe and secure information society for Eswatini; and strengthen co-operation, collaboration and partnerships on cybersecurity.

G. Initiatives to combat cybercrime
- Eswatini is one of the 195 INTERPOL [295] member countries.[296]
- Establishment of the National Cybersecurity Advisory Council[297] to render support and provide advice on cyber affairs in the country.
- Review of its National Information and Infrastructure and Communication Policy,[298] which 'discusses the government's measures to implement ICT initiatives that are aimed at facilitating the development of the country'. It considers the need for a reform of the cybersecurity status so as to stay abreast of recent developments and cyber threats.
- Establishment of the Eswatini National Cybersecurity Awareness Month initiative.

14. Fiji

A. National cyber threat landscape
There is no cyber threat landscape assessment rating for Fiji on the National Cyber Security Index (NCSI).

B. National cybercrime legislation and related laws
- Cybercrime Act[299]
- Crimes Act 2009[300]

293 SZCIRT, 'Who We Are', available at: https://ncsirt.org.sz/who-we-are/
294 Eswatini National Cybersecurity Strategy, available at: www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Eswatini%20NCS%202020.pdf (accessed 13 January 2023).
295 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
296 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).
297 National Cybersecurity Advisory Council, available at: www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Eswatini%20NCS%202020.pdf (accessed 23 January 2023).
298 National Information and Infrastructure and Communication Policy, available at: https://tradecca.thecommonwealth.org/pdf/national-information-and-infrastructure-and-communication-policy-implementation-plan-2012-2016 (accessed 23 January 2023).
299 Cybercrime Act 2021, Laws of Fiji, available at: https://laws.gov.fj/Acts/DisplayAct/3165 (accessed 18 January 2023).
300 Crimes Act 2009, Laws of Fiji, available at: https://laws.gov.fj/Acts/DisplayAct/3164 (accessed 18 January 2023).

C. Scope/application of laws
- The Cybercrime Act addresses cybercrime by prescribing computer-related and content-related offences, requirements in the collection of electronic evidence, and remedies in relation to cybercrime. It provides for offences such as computer-related fraud, forgery and extortion, and identity theft.
- The Crimes Act repeals the Penal Code and makes comprehensive provisions relating to criminal responsibility and criminal offences. Part 17, Division 6, of the Act[301] provides for computer offences such as unauthorised access, modification or impairment of electronic communication, unauthorised access to restricted data, and serious computer offences.

D. National computer emergency response team (CERT)/computer security incident response team (CSIRT)
Fiji does not currently have an officially recognised CERT/CSIRT.

E. National cybersecurity strategy
The Fiji Government does not have a designated national cybersecurity strategy.

F. Initiatives to combat cybercrime
- Fiji was invited to accede to the Convention on Cybercrime (ETS No. 185)[302] in 2021.
- Fiji is one of the 195 INTERPOL [303] member countries.[304]
- Fiji participates in international initiatives and offers cybersecurity services. These initiatives include being a member of the International Telecommunication Union–IMPACT,[305] and cybersecurity forums like the Asia Pacific CIRT and Pacific Regional PacCERT (Pacific Computer Emergency Incidents Response Team).
- Creation of agencies such as the Finance Intelligence Unit (FIU),[306] which investigates cyber offences like cyber laundering, and the Cybersecurity Working Group, which is a cybercrime unit within the police force.

15. Gabon

A. National cyber threat landscape
There is no cyber threat landscape assessment rating for Gabon on the National Cyber Security Index (NCSI).

B. National cybercrime legislation and related laws
- Ordinance No. 15/PR/2018 of 23 February 2018 on the Regulation of Cybersecurity and the Fight against Cybercrime[307]

301 Ibid, sections 336–346.
302 Council of Europe, 'The Budapest Convention (ETS No. 185) and is Protocols', available at: www.coe.int/en/web/cybercrime/the-budapest-convention (accessed 26 January 2023).
303 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
304 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).
305 ITU (2016), ICB4PAC Project, available at: www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/ICB4PAC/Pages/default.aspx (accessed 15 January 2023).
306 Fiji Financial Intelligence Unit, Home, available at: www.fijifiu.gov.fj/ (accessed 31 January 2023).
307 Ordinance No. 15/PR/2018 of 23 February 2018 on Cybersecurity and Cybercrime, available at: http://www.droit-afrique.com/uploads/Gabon-Ordonnance-2018-15-cybersecurite-cybercriminalite.pdf (accessed 13 January 2023).

- Law No. 001/2011 on the Protection of Personal Data (Loi N°001/2011 relative à la protection des données à caractère personnel)[308]
- Law No. 025/2021 of 28 December 2021 Regulating Electronic Transactions in Gabon ('Electronic Transactions Law')[309]
- Law No. 26/2018 of 22 October 2018 regarding Electronic Communications in Gabon (Loi N° 026/2018 du 17/10/2019 portant réglementation des communications électroniques en République Gabonaise)[310]
- Constitution de la République Gabonaise[311]
- Regulation No. 01/CEMAC/UMAC/CM of 4th April 2003 relating to the Prevention and Suppression of Money Laundering and Financing of Terrorism in Central Africa[312]
- Order No. 00000014/PR/2018 of February 23, 2018 on the Regulation of Electronic Transactions in the Gabonese Republic

C. Scope/application of laws

- Ordinance No. 15/PR/2018 of 23 February 2018 on Cybersecurity and Cybercrime[313] provides the background for general cybersecurity policies and lays down the obligations for actors, including the service providers. It is the main legal text related to cybercrime, both for substantive law and procedural powers, as well as basic provisions on international co-operation.
- The Electronic Transactions Law provides the terms and conditions applicable to electronic transactions, as well as a framework for the measures that must be put in place to guarantee the integrity, confidentiality and security of data by providers of electronic communications and technical services for securing electronic transactions.[314] It also sets out specific rules for e-commerce, distance contracts, electronic marketing, and administrative acts or contracts carried out through electronic means.[315]
- Law No. 001/2011 on the Protection of Personal Data[316] sets up the rules that guide the collection, processing, use, or disposal, transmission and storage of personal data.

D. National computer emergency response team (CERT)/computer security incident response team (CSIRT)

ITU conducted a CIRT assessment for Gabon in 2010. However, as at the time of this research, Gabon was not included among the countries that have a computer security incident response team[317] as it is yet to operate a national-level CERT: No specialised cybercrime investigation or prosecution authorities have been reported as operational in Gabon or available via public sources.

---

308 *Loi n°001/2011 relative à la protection des données à caractère personnel*, available at: www.afapdp.org/archives/110/gabon-loi-relative-a-la-protection-des-donnees-personnelles-du-4-mai-2011-2 (accessed 13 January 2023).

309 Law No. 025/2021 of 28 December 2021 Regulating Electronic Transactions in Gabon, available at: http://journal-officiel.ga/18190-025-2021-/ (accessed 13 January 2023).

310 *Loi n° 026/2018 du 17/10/2019 portant réglementation des communications électroniques en République Gabonaise*, available at: http://journal-officiel.ga/5055-026-2018-/ (accessed 13 January 2023).

311 *Constitution de la République Gabonaise*, available at: http://journal-officiel.ga/constitution (accessed 12 January 2023).

312 Regulation No. 01/CEMAC/UMAC/CM of 4 April 2003 on the Prevention and Suppression of Money Laundering and Financing Terrorism in Central Africa, available at: www.anif.cm/images/pdfanif/CEMAC_Regulation.pdf (accessed 12 January 2023).

313 Ordinance No. 15/PR/2018 of 23 February 2018 on Cybersecurity and Cybercrime, available at: http://www.droit-afrique.com/uploads/Gabon-Ordonnance-2018-15-cybersecurite-cybercriminalite.pdf (accessed 13 January 2023).

314 DataGuidance (2021), Gabon – Data Protection Overview, 14 July, available at: www.dataguidance.com/notes/gabon-data-protection-overview (accessed 14 January 2023).

315 Law No. 025/2021 of 28 December 2021 Regulating Electronic Transactions in Gabon, available at: http://journal-officiel.ga/18190-025-2021-/ (accessed 13 January 2023).

316 Law No. 001/2011 on the Protection of Personal Data, available at: www.afapdp.org/archives/110/gabon-loi-relative-a-la-protection-des-donnees-personnelles-du-4-mai-2011-2 (accessed 13 January 2023).

317 Africa CERT, African CSIRTs, available at: www.africacert.org/african-csirts/ (accessed 14 January 2023).

E. National cybersecurity strategy
Gabon is yet to adopt an officially recognised national cybersecurity strategy.

F. Initiatives to combat cybercrime
- Gabon is one of the 195 INTERPOL [318] member countries.[319]
- The establishment of the National Agency for Digital Infrastructure and Frequencies (ANINF), which is the officially recognised agency responsible for implementing a national cybersecurity strategy, policy and roadmap in Gabon.

16. The Gambia

A. National cyber threat landscape
Exact statistics and data on cybercrime are not readily available on The Gambia;[320] however, according to the National Cyber Security Index (NCSI), [321] as of January 2023 Gambia ranked: 143rd on the NCSI with a score of 11.69. The Gambia was also identified as vulnerable, as many computer-related crimes have been charged using general economic crime-related regulations.[322]

B. National cybercrime legislation and related laws
- Information and Communications Act 2008 ('the IC Act')[323]
- Gambia Cybercrime Bill

C. Scope/application of laws
The IC Act provides for the regulation of information communication, while protecting against computer misuse and cybercrime, child pornography, and unauthorised reprogramming of telecommunication. Part III, sections 163 to 173 of the Act provide for offences such as: unauthorised access to computer data, unauthorised modification of computer material, publishing of information which is obscene in electronic form, and computer-related extortion, fraud and forgery.

D. Sanctions/penalties for cyber-related crimes
Anybody who commits an offence under Part III of the IC Act, is liable on conviction to a fine of 200,000 dalasi or imprisonment for a term of five years, or to both fine and imprisonment; while a body corporate will be liable to a fine of not less than 500,000 dalasi. Further, the penalty on conviction for child pornography is imprisonment for life.[324]

E. National computer emergency response team (CERT)/computer security incident response team (CSIRT)
The Gambia Computer Security and Incident Response Team.[325]

---

318 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
319 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).
320 Symantec and African Union Commission (2016), *Cyber Crime and Cyber Security Trends in Africa*, November, available at: https://securitydelta.nl/media/com_hsd/report/135/document/Cyber-security-trends-report-Africa-en.pdf (accessed 4 January 2023).
321 NCSI Gambia, available at: https://ncsi.ega.ee/country/gm/ (accessed 3 March 2023).
322 'Reform of cybercrime legislation: The Gambia', available at: https://rm.coe.int/cyber-eu-coe-webinar-africa-en-july-2020-momodou/16809ef01e (accessed 6 January 2023).
323 Information and Communications Act 2008, available at: https://ictpolicyafrica.org/api/documents/download?_id=5d8070601c3577001bda40d1 (accessed 14 January 2023).
324 Information and Communications Act 2008, section 174, available at: https://ictpolicyafrica.org/api/documents/download?_id=5d8070601c3577001bda40d1 (accessed 14 January 2023).
325 The Gambia Computer Security and Incident Response Team, available at: https://gmcsirt.gm/ (accessed 14 January 2023).

F. National cybersecurity strategy
The National Cybersecurity Policy, Strategy and Action Plan (2020–2024) identifies and assesses cyber threats, while proffering effective countermeasures and an action plan to entrench cybersecurity in the country. Under this plan,[326] four strategies are formulated:
- understanding the cybersecurity risk;
- controlling the risk;
- organising and mobilising for cybersecurity; and
- institutional and policy build-up.

G. Initiatives to combat cybercrime
- The Gambia is one of the 195 INTERPOL [327] member countries.[328]
- Cybersecurity efforts in The Gambia are led by the Ministry of Information and Communications Infrastructure.
- The government has embarked on several initiatives in combatting cybercrime in the country. These include reform of cybercrime legislation to meet the evolving cyber threats, establishment of specialised agencies to tackle cybercrime and other related crimes in the country, creation of sectoral CSIRT focal points and the handover of a cybercrime laboratory by ECOWAS.[329]
- Gambia recently ratified the African Union Convention on Cyber Security and Personal Data Protection 2014 ('the Malabo Convention') and deposited its instrument of ratification with the African Union Commission in December 2022.

17. Ghana

A. National cyber threat landscape
According to the National Cyber Security Index (NCSI),[330] as of January 2023 Ghana ranked: 98th on the NCSI with a score of 31.17; 43rd on the Global Cybersecurity Index; 116th on the ICT Development Index; and 96th on the Networked Readiness Index.

B. National cybercrime legislation and related laws
- Electronic Transactions Act (ETA) 2008[331]
- Electronic Communication Act 2008 Act No. 775[332]
- Economic and Organised Crime Act 2010 (EOCA)[333]
- Ghana National Information Technology Agency Act 2008[334]
- Data Protection Act (DPA) 2012[335]

326 The Gambia National Cyber Security Strategy and Action Plan 2020–2024 , available at: https://unidir.org/cpp/en/state-pdf-export/eyJjb3VudHJ5X2dyb3VwX2lkIjoiMjAifQ (accessed 13 January 2023).
327 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
328 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).
329 Economic Community of West African States (ECOWAS), available at: https://ecowas.int/ (accessed 27 January 2023).
330 NCSI: Ghana, available at: https://ncsi.ega.ee/country/gh/ (accessed 14 January 2023).
331 Electronic Transactions Act No. 772, available at: www.researchictafrica.net/countries/ghana/Electronic_Transactions_Act_no_772:2008.pdf (accessed 13 January 2023).
332 Electronic Communications Act, available at: https://nita.gov.gh/theevooc/2017/12/Electronic-Communications-Act-775.pdf (accessed 13 January 2023).
333 Economic and Organised Crime Act 2010, available at: www.parliament.gh/epanel/docs/bills/Economic%20and%20Organised%20Crime%20Act%202010%20Act%20804.pdf#viewer.action=download (accessed 13 January 2023).
334 National Information Technology Agency Act, available at: https://nita.gov.gh/theevooc/2017/12/National-Information-Technology-Agency-Act-771.pdf (accessed 13 January 2023).
335 Data Protection Act, available at: https://nita.gov.gh/wp-content/uploads/2017/12/Data-Protection-Act-2012-Act-843.pdf (accessed 13 January 2023).

- Anti-Money Laundering Act 2008 (AMLA)[336]
- Mutual Legal Assistance Act 2010 (MLAA)[337]

C. Scope/application of laws

- The ETA provides for the regulation of electronic communications, related transactions and connected purposes.[338] Sections 107 to 136 of the ETA provide for cyber offences which include: electronic trafficking; forgery; fraudulent electronic fund transfer;[339] general cyber offences;[340] unauthorised access or interception;[341] unauthorised interference with an electronic record;[342] unauthorised access to devices;[343] unauthorised access to a computer program or electronic record;[344] unauthorised modification of a computer program or electronic record;[345] unauthorised disclosure of an access code;[346] and child pornography.[347]
- The ECA provides for the regulation of electronic communications, the regulation of broadcasting, the use of the electromagnetic spectrum and for related matters. Section 73 of the ECA provides for offences such as the unauthorised interception of electronic communications and stealing of transmitted messages or data.
- The EOCA establishes the Economic and Organised Crime Office as a specialised agency to monitor and investigate economic and organised crime, prosecute offences to recover the proceeds of crime, and for related matters.
- The DPA ensures protection of personal data.
- The MLAA provides for the implementation of agreements or other arrangements for mutual legal assistance in respect of criminal matters and to provide for related matters.

D. Sanctions/penalties for cyber-related crimes

- The penalty for the cyber-related offences contained in the ETA range from a fine of not more than 2,500 hundred penalty units[348] to 10,000 penalty units or to a term of imprisonment of not more than 5 to 20 years, or to both. Also, the court can make an order of confiscation of assets derived from the commission of the offence.[349] And a conviction shall not limit the right of a complainant to bring a civil action.[350]
- Sanctions for committing an offence under the ECA will cause liability on summary conviction, to a fine of not more than 3,000 penalty units or to a term of imprisonment of not more than 5 years, or to both. However, where the offence is committed by a corporate entity, that entity is liable to a fine of not more than 9,000 penalty units and each director of that entity shall be deemed to have committed the offence.

E. National computer emergency response team (CERT)/computer security incident response team (CSIRT)

---

336 Anti-Money Laundering Act 2008, available at: https://fic.gov.gh/wp-content/uploads/2015/11/AML-Act-2008-Act-749.pdf (accessed 13 January 2023).
337 Mutual Legal Assistance Act 2010, available at: http://elibrary.jsg.gov.gh/fg/laws%20of%20ghana/2%20REP/MUTUAL%20LEGAL%20ASSISTANCE%20ACT,%202010%20ACT%20807.htm (accessed 14 January 2023).
338 Electronic Transactions Act No. 772, section 1, available at: www.researchictafrica.net/countries/ghana/Electronic_Transactions_Act_no_772:2008.pdf (accessed 13 January 2023).
339 Ibid, section 122.
340 Ibid, section 123.
341 Ibid, section 124.
342 Ibid, section 125.
343 Ibid, section 126.
344 Ibid, section 130.
345 Ibid, section 131.
346 Ibid, section 132.
347 Ibid, section 136.
348 Penalty units are a standard amount of money used to calculate fines for offences.
349 Ibid, section 137.
350 Ibid, section 140.

Ghana has established a Ghana National CERT (CERT-GH)[351] under the authority of the Ministry of Communications and Digitalisation. CERT-GH serves as the country's focal point for computer security incident response, with various sectoral-level CERTs which co-ordinate on technical expertise and exercise domain-specific authorities to help secure critical infrastructure within their sectors from cyberattacks.

F. National cybersecurity strategy

The Ghana National Cyber Security Policy and Strategy[352] has eight pillars: effective governance; a legislative and regulatory framework; research and development towards self-reliance; cybersecurity emergency readiness; a cybersecurity technology framework; a culture of security and capacity building; compliance and enforcement; as well as international co-operation.

G. Initiatives to combat cybercrime

- Ghana ratified the Convention on Cybercrime (ETS No. 185)[353] on 3 December 2018; it came into force in the country on 1 April 2019.[354]
- Ghana acceded to the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224) on 28 June 2023.[355]
- Ghana has ratified the African Union Convention on Cyber Security and Personal Data Protection 2014 ('the Malabo Convention').
- Ghana is one of the 195 INTERPOL [356] member countries.[357]
- Establishment of the National Cyber Security Centre (NCSC),[358] which ensures cybercrime reporting for a resilient and secure cyberspace and promotion of cybersecurity in the country.
- Initiatives such as creation of a National Cyber Crime Awareness Program, a National Cyber Security Crisis Management Plan, and the drafting and review of the Ghana National Cyber Security Policy.[359]
- Facilitation of National Cybersecurity Awareness Month,[360] to 'Build synergies among all relevant stakeholders, ensure compliance with cybersecurity regulations, and enhance public–private sector understanding of cybersecurity regulations'. The National Cyber Security Awareness Month (NCSAM) 2022 took place in October across the country under the theme 'Regulating Cybersecurity: A Public–Private Sector Collaborative Approach'.[361]
- Allocation of a dedicated budget for cybersecurity and cybercrime developments in the country.
- The National Communication Authority is the statutory body mandated to licence and regulate electronic communications activities and services in the country. However, there are 'several agencies within the Government of Ghana that share responsibility for cybersecurity, including the National Communications Authority (Telecom Regulator), National Information Technology Agency (ICT Regulator), Ministry of Information and Communications Technology, and the Ghanaian National Security Agency'.

351 Ghana National CERT (CERT-GH), available at: https://cybersecurity.gov.gh/cert (accessed 13 January 2023).
352 National Cyber Security Policy Strategy, available at: www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/National-Cyber-Security-Policy-Strategy-Revised_23_07_15.pdf (accessed 13 January 2023).
353 Council of Europe, 'The Budapest Convention (ETS No. 185) and is Protocols', available at: www.coe.int/en/web/cybercrime/the-budapest-convention (accessed 26 January 2023).
354 Council of Europe, 'Complete list of Council of Europe's treaties', Treaty Office, available at: www.coe.int/en/web/conventions/full-list (accessed 25 January 2023).
355 https://www.csa.gov.gh/ghana-signs-council-of-europe-second-additional-protocol-to-the%20-convention-on-cybercrime
356 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
357 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).
358 National Security Authority, available at: www.csa.gov.gh/ (accessed 27 January 2023).
359 National Cyber Security Policy, available at: www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/National-Cyber-Security-Policy-Strategy-Revised_23_07_15.pdf (accessed 25 January 2023).
360 NCSAM 2022, available at: https://ncsam.csa.gov.gh/ (accessed 27 January 2023).
361 Ibid.

- Creation of specialised institutions such as: the National Information Technology Agency (NITA), the Ghana Financial and Economic Crimes Court (FECC), the National Security Council (NSC), the cybercrime unit in the Criminal Investigations Division (CID) of the Ghana Police Service, the Bureau of National Investigations (BNI), the Economic and Organized Crime Office (EOCO),[362] and the Ghana Financial Intelligence Centre (FIC).[363]

18. Grenada

A. National cyber threat landscape
According to the National Cyber Security Index (NCSI),[364] as of January 2023 Grenada ranked: 118th out of 161 countries on the NCSI with a score of 20.78; 163rd out of 194 countries on the Global Cybersecurity Index; and 73rd on the ICT Development Index.

B. National cybercrime legislation and related laws
- Electronic Crimes Act 2013[365]

C. Scope/application of laws
The Electronic Crimes Act seeks to provide for the prevention and punishment of electronic crimes. Part II thereof provides for cyber offences such as access and interference, sending offensive messages through a communications service, identity theft, electronic defamation, electronic forgery, electronic fraud, sending of malicious code, misuse of encryption, child pornography, electronic terrorism, electronic stalking, spoofing and unauthorised access to a code.

D. Sanctions/penalties for cyber-related crimes
The contravention of the Electronic Crimes Act will make a person liable on conviction to a fine between 50,000 and 300,000 Eastern Caribbean dollars or to a term of imprisonment between 1 and 20 years, or to both fine and imprisonment.

E. National computer emergency response team (CERT)/computer security incident response team (CSIRT)
Grenada does not have an officially recognised national CERT/CSIRT.

F. National cybersecurity strategy
Grenada does not have an officially recognised national cybersecurity strategy.

G. Initiatives to combat cybercrime
- Grenada is a member of the Caribbean Community (CARICOM) and receives support from IMPACS in addressing cyberthreats and vulnerabilities. As a member state, Grenada also signed off on the CARICOM Cyber Security and Cybercrime Action Plan (CCSCAP).
- Grenada is one of the 195 INTERPOL [366] member countries.[367]
- Grenada has a specialised unit for combatting cybercrime. The unit also conducts digital forensics.
- International co-operation and collaboration, to ensure information flow on combatting cybercrime.

362 Economic and Organised Crime Office, available at: https://eoco.gov.gh/faq/ (accessed 23 January 2023).
363 FIC, Home, available at: https://fic.gov.gh/ (accessed 27 January 2023).
364 NCSI: Grenada, available at: https://ncsi.ega.ee/country/gd/ (accessed 17 January 2023).
365 Electronic Crimes Act, available at: https://nowgrenada.com/wp-content/uploads/2013/07/Electronic-Crimes-Bill.pdf?x65460 (accessed 16 January 2023).
366 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
367 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).

19. Guyana

A. National cyber threat landscape

According to the National Cyber Security Index (NCSI),[368] as of January 2023 Guyana ranked: 147th out of 161 countries on the NCSI with a score of 10.39; 114th out of 194 countries on the Global Cybersecurity Index; 124th on the ICT Development Index; and 100th on the Networked Readiness Index.

B. National cybercrime legislation and related laws

- Cybercrime Act 2018[369]
- Electronic Communications and Transactions Bill 2018[370]
- Interception of Communications Act, No. 21 of 2008[371]

C. Scope/application of laws

- The Cybercrime Act, passed in 2018, contains substantive cybercrime provisions. The Cybercrime Act combats cybercrime by creating cyber offences, prescribing their penalties, and through investigation and prosecution of the offences. Part II of the Act provides for cyber offences such as illegal access to a computer system, illegal interception, illegal data and system interference, unauthorised access to electronic data, computer-related forgery and fraud, identity-related offences, child pornography and luring, and using a computer system to harass or humiliate a person. These are followed by provisions criminalising offences affecting critical infrastructure and content-related offences.
- The Electronic Communications and Transactions Bill provides for the facilitation and regulation of secure electronic communications and transactions and for their legal recognition.
- The Interception of Communications Act provides for the interception of communications, acquisition and disclosure of data relating to communications, and the means by which protected communications may be accessed.

D. Sanctions/penalties for cyber-related crimes

- Contravention of the Cyber Crimes Act will make a person liable on conviction to a fine between 3 million and 10 million Guyana or to a term of imprisonment between 3 and 10 years, or to both fine and imprisonment.
- Section 3 of the Interception of Communications Act provides that 'a person who intentionally intercepts a communication in the course of its transmission by means of a telecommunication system commits an offence and is liable to the summary conviction to a fine not exceeding five million dollars and to imprisonment for a term not exceeding three years'.

E. National computer emergency response team (CERT)/computer security incident response team (CSIRT)

The Guyana National Computer Incidents Response Team (CIRT-GY) is the national computer incident response team that provides technical assistance to public agencies to prevent and respond effectively to information security incidents of national importance. The team initially functioned as a unit within the Ministry of Home Affairs, until 30 September 2016. Guyana National CIRT is now under the purview of the National Data Management Authority (NDMA) within the Office of the Prime Minister.[372]

368 NCSI: Guyana, available at: https://ncsi.ega.ee/country/gy/ (accessed 17 January 2023).
369 Cyber Crime Act 2018, Parliament of Guyana, available at: https://parliament.gov.gy/publications/acts-of-parliament/cyber-crime-act-2018 (accessed 18 January 2023).
370 Electronic Communications and Transactions Bill, available at: https://f.hubspotusercontent00.net/hubfs/8779058/delete-technology-2021/pdf/Electronic_Communications_and_TransactionsBill_2018.pdf (accessed 16 January 2023).
371 Interception of Communication Act 2008, Parliament of Guyana, available at: https://parliament.gov.gy/publications/acts-of-parliament/interception-of-communication-act-2008 (accessed 18 January 2023).
372 Guyana Cybercrime Policies and Strategies, available at: https://www.coe.int/en/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/guyana?_101_INSTANCE_CmDb7M4RGb4Z_viewMode=view/ (accessed 3 March 2023).

F. National cybersecurity strategy

At the time this research was carried out, Guyana had not yet adopted an officially recognised national cybersecurity strategy. A consultation on the development of such a strategy began in 2019, facilitated through a collaboration between the National Data Management Authority (NDMA) of Guyana and the Organization of American States (OAS).

G. Initiatives to combat cybercrime

- Guyana is a member of the Caribbean Community (CARICOM) and receives support from IMPACS in addressing cyberthreats and vulnerabilities. As a member state, Guyana also signed off on the CARICOM Cyber Security and Cybercrime Action Plan (CCSCAP).
- Guyana is one of the 195 INTERPOL [373] member countries.
- The Government of Guyana has stated its intention and interest in creating a forum to enhance government co-ordination in combatting cybercrime.
- The Cybersecurity Division of the National Data Management Authority[374] focuses on safeguarding the confidentiality, integrity and availability of the Government of Guyana's ICT infrastructure, together with its services, applications and data.
- The institutionalisation of a Cyber Security Awareness Month with programmes to raise awareness on cybersecurity.[375]

20. India

A. National cyber threat landscape

According to the National Cyber Security Index (NCSI),[376] as of January 2023 India ranked: 50th out of 161 countries on the NCSI with a score of 59.74; 10th out of 194 countries on the Global Cybersecurity Index; 134th on the ICT Development Index; and 67th on the Networked Readiness Index.Like many countries, India is suffering increasingly from cybercrime. According to 2023 cybercrime statistics:[377] 'the number of cyber-related crimes reported in 2018 was 208,456. In the first 2 months of 2022 alone, there were a reported 212,485 cybercrimes, more than the entirety of 2018. The figures rose more sharply through the pandemic, with reported crime jumping from 394,499 cases in 2019 to 1,158,208 in 2020 and 1,402,809 in 2021. Between Q1 and Q2 2022, cybercrime across India increased by 15.3%.'

B. National cybercrime legislation and related laws

- The India Information Technology Act of 2000[378]
- The Indian Penal Code[379]

C. Scope/application of laws

- The Information Technology Act is the principal legislation on cybercrime in India. It provides for the use of electronic and digital signatures, and the authentication of electronic records. It also makes provisions for cybercrimes and computer-related offences like identity theft, unlawful access to a computer system, cyber terrorism and impersonation using a computer resource.

373 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
374 Available at: https://ndma.gov.gy/cybersecurity-advisory-update-global-ransomware-attack/
375 National Data Management Authority, available at: https://ndma.gov.gy/ (accessed 04 March 2023).
376 NCSI: India, available at: https://ncsi.ega.ee/country/in/ (accessed 17 January 2023).
377 'The Latest 2023 Cyber Crime Statistics', available at: https://aag-it.com/the-latest-cyber-crime-statistics/ (accessed 9 January 2023).
378 Information Technology Act 2000, available at: http://indiacode.nic.in/handle/123456789/1999 (accessed 18 January 2023).
379 Penal Code, available at: https://legislative.gov.in/sites/default/files/A1860-45.pdf (accessed 16 January 2023).

D. Sanctions/penalties for cyber-related crimes
The Information Technology Act provides for cyber offences such as cyber terrorism. Section 43 of the Act provides for penalties and compensation for damage to a computer or computer system. Section 66 provides for computer-related offences, which are 'punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both'. Further, section 66F prescribes that 'cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life'.

E. National computer emergency response team (CERT)/computer security incident response team (CSIRT)
The Indian Computer Emergency Response Team (CERT-In) oversees incident response, which includes cybersecurity analyses, predictions and warnings.

F. National cybersecurity strategy
There is a National Cyber Security Strategy 2020, which was submitted by the Data Security Council of India,[380] and a National Cyber Security Strategy 2021, which was formulated by the National Security Council Secretariat.[381] They serve as guides to tackle cybersecurity across various parameters, including strengthening national resources, and building local capabilities and national cyber audit standards.

G. Initiatives to combat cybercrime
- India is one of the 195 INTERPOL [382] member countries.[383]
- Implementation of the country's National Cyber Security Policy in 2013, with the objective of 'protecting information and information infrastructure in cyberspace, build capabilities to prevent and respond to cyber threats, reduce vulnerabilities, and minimise the damage caused by cyber incidents'.
- The government also facilitates awareness programmes on cyber threats and forms of cybercrimes. Alerts and advisories are given where appropriate, with law enforcement and other security personnel trained from time to time. For instance, ICERT[384] issues alerts and advisories to keep people updated on the latest cyber threats, security measures and safe usage of digital technologies.[385] There is also the MyGov platform and the Digital India Platform for creating information security awareness.
- Creation of an online cybercrime reporting site[386] to make sure cybercrime incidents are easily reported in the country. The use of a toll-free number to lodge complaints also ensures a higher level of accessibility for the public. Further, a Citizen Financial Cyber Fraud Reporting and Management System exists to encourage the immediate reporting of financial fraud.
- Creation of the Indian Cyber Crime Coordination Centre (I4C)[387] to specifically address and provide awareness on cyber threats, cybercrime and related offences in the country. Joint Cyber Coordination Teams have also been constituted for seven regions to 'address the issue of jurisdictional complexity, and provision of a robust coordination framework'.[388]

380 Data Security Council India National Cyber Security Strategy, available at: https://www.dsci.in/sites/default/files/documents/resource_centre/National Cyber Security Strategy 2020 DSCI submission.pdf
381 Available at: https://government.economictimes.indiatimes.com/news/secure-india/national-cyber-security-strategy-2021-draft-formulated-by-nscs-mos-it-rajeev-chandrasekhar/90602963?redirect=1
382 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
383 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).
384 ICERT, Ministry of Electronics and Information Technology, Government of India, available at: www.meity.gov.in/content/icert (accessed 31 January 2023).
385 Prevention of Cyber Crimes, available at: https://pib.gov.in/pib.gov.in/Pressreleaseshare.aspx?PRID=1845321 (accessed 25 January 2023).
386 *Cybercrime Report*, available at: http://www.cybercrime.gov.in/ (accessed 26 January 2023).
387 Ministry of Home Affairs, Details about Indian Cybercrime Coordination Centre (I4C) Scheme, available at: www.mha.gov.in/division_of_mha/cyber-and-information-security-cis-division/Details-about-Indian-Cybercrime-Coordination-Centre-I4C-Scheme (accessed 31 January 2023).
388 Prevention of Cyber Crimes, available at: https://pib.gov.in/pib.gov.in/Pressreleaseshare.aspx?PRID=1845321 (accessed 25 January 2023).

- Establishment of the National Security Council Secretariat in India, which serves as the main governmental institution for improving cybersecurity in the country.
- Formulation of a Cyber Crisis Management Plan to respond to cyber incidents, along with facilitation of cybersecurity audits and mock drills through CERT-In to ensure the continuous readiness of organisations and critical sectors of the country.[389]
- The Government of India, through the Ministry of Home Affairs, has implemented the Cybercrime Prevention against Women and Children Scheme. The scheme aims to prevent, or at the least reduce, incidents of cybercrime against these groups. Financial assistance is provided, while cyber forensic and training laboratories have been commissioned in about 28 states in the country.[390]
- Facilitation of co-ordinated, collaborative and consistent security programmes; for instance, the Ministry of Electronics and Information Technology[391] co-ordinates programmes and disseminates information security tips through websites such as: www.infosecawareness.in[392] and www.csk.gov.in.[393] Cyber activities are also co-ordinated during Cyber Security Awareness Month in October and Safe Internet Day (which was 8 February in 2022).

21. Jamaica

A. National cyber threat landscape

According to the National Cyber Security Index (NCSI),[394] as of January 2023 Jamaica ranked: 81st out of 161 countries on the NCSI with a score of 41.56; 106th out of 194 countries on the Global Cybersecurity Index; 98th on the ICT Development Index; and 74th on the Networked Readiness Index.

B. National cybercrime legislation and related laws

- Cybercrimes Act 2010[395]
- The Child Pornography (Prevention) Act 2009[396]
- Criminal Justice (Suppression of Criminal Organizations) Act 2014[397]
- Computer Misuse Act 2006

C. Scope/application of laws

- The Cybercrimes Act provides criminal sanctions for the misuse of computer systems or data and the abuse of electronic transactions, and facilitates the investigation and prosecution of cybercrimes. It provides for cyber offences such as illegal access, unauthorised obstruction of computer operation, data interference, system interference, misuse of devices, and unauthorised interception of function and service.

389 Ibid.
390 Ibid.
391 Ministry of Electronics and Information Technology, Government of India, Home, available at: www.meity.gov.in/ (accessed 31 January 2023).
392 Information Security Education and Awareness (ISEA), available at: www.infosecawareness.in/ (accessed 31 January 2023).
393 Cyber Swachhta Kendra, available at: www.csk.gov.in/ (accessed 31 January 2023).
394 NCSI: Jamaica, available at: https://ncsi.ega.ee/country/jm/ (accessed 17 January 2023).
395 Cybercrimes Act 2010, available at: www.japarliament.gov.jm/attachments/341_The%20Cybercrimes%20Act,%202010.pdf (accessed 15 January 2023).
396 Child Pornography (Prevention) Act 2009, available at: https://japarliament.gov.jm/attachments/341_The%20Child%20Pornography%20Act.pdf (accessed 15 January 2023).
397 Jamaica – Criminal Justice (Suppression of Criminal Organizations) Act 2014 (Act No. 3 of 2014), available at: http://ilo.org/dyn/natlex/natlex4.detail?p_lang=en&p_isn=98287&p_country=JAM&p_count=217 (accessed 18 January 2023).

- The Child Pornography (Prevention) Act prohibits the production, distribution, importation, exportation or possession of child pornography, and the use of children for child pornography, and connected matters. The Act provides for the offence of using or involving a child in the production of child pornography, possessing or knowingly accessing child pornography, and distributing child pornography.

D. Sanctions/penalties for cyber-related crimes

- Contravention of the Cybercrimes Act will make a person liable on conviction to a fine between two and three million Jamaican dollars or to a term of imprisonment between two and seven years, or to both fine and imprisonment.
- The punishment under the Child Pornography (Prevention) Act on conviction on indictment before a circuit court, will make a person liable to a fine or to imprisonment for a term ranging from 15 to 20 years, or to both such fine and imprisonment. It further prescribes a fine or imprisonment not exceeding 20 years, or to both such fine and imprisonment, where a body corporate is found liable.

E. National computer emergency response team (CERT)/computer security incident response team (CSIRT)

The Jamaica Cyber Incident Response Team (JaCIRT) is a division under the Ministry of Science, Energy and Technology. It supports the secure operation of the information technology resources of the Government of Jamaica (GOJ) by co-ordinating incident response for the ministries, agencies and departments of the GOJ, and also provides other support necessary to protect the nation's IT assets from cyberattacks.[398]

F. National cybersecurity strategy

The Jamaica National Cybersecurity Strategy[399]seeks to establish 'a framework built around the following key areas: Technical Measures; human resource and capacity building; legal and regulatory; and public education and awareness'.[400] Importantly, it seeks to: create 'awareness regarding cybersecurity; and develop a culture of cybersecurity'. It is believed that the strategy will ultimately engender confidence in cyberspace such that Jamaicans can continue to achieve their full potential.[401]

G. Initiatives to combat cybercrime

- Jamaica is a member of the Caribbean Community (CARICOM). Jamaica has led many CARICOM cybercrime initiatives, including advancing CARICOM's objectives at the UN Ad Hoc Committee process to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes.[402]
- Jamaica is one of the 195 INTERPOL [403] member countries.[404]
- The establishment of the National Cybersecurity Task Force (NCSTF), which includes stakeholders from different sectors. The NCSTF is tasked with ensuring that quality and skilled cyber talent exists in the country's workforce, while enhancing the country's cyberspace.

398 Government of Jamaica, About Jamaica CIRT, Cyber Incident Response Team, available at: https://www.cirt.gov.jm/page/about-jamaica-cirt

399 Jamaica National Cybersecurity Strategy, available at: www.mset.gov.jm/wp-content/uploads/2019/09/Jamaica-National-Cyber-Security-Strategy-2015.pdf (accessed 26 January 2023).

400 Ibid.

401 Jamaica National Cybersecurity Strategy, available at: www.mset.gov.jm/wp-content/uploads/2019/09/Jamaica-National-Cyber-Security-Strategy-2015.pdf (accessed 26 January 2023).

402 PublicTechnology.net (2022), 'No one is an island: how Caribbean states are working together to tackle cybercrime', 17 October, available at: https://publictechnology.net/articles/features/no-one-island-how-caribbean-states-are-working-together-tackle-cybercrime (accessed 24 January 2023).

403 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).

404 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).

- The establishment of the Cyber Forensics and Risk Management Unit, which surveys cyber threats, conducts cyber forensics and vulnerability assessments, and ensures secured cyber operations.
- The upscaling and upskilling of law enforcement officers and prosecutors. In this regard, the government has created dedicated units such as the Communication Forensics and Cybercrime Unit (CFCU) within the Jamaica Constabulary Force (JCF)[405] and the Digital Evidence and Cybercrimes Unit in the Office of the Director of Public Prosecution (ODPP).[406] These provide the necessary assistance for investigation of crimes and preparation of evidence.
- Other initiatives and policies[407] to combat cybercrime in Jamaica include: the national ICT Strategy 2007–2012; the National Development Plan 2030 ('Vision 2030 Jamaica');[408] the ICT Policy 2011; and the National Security Policy 2014,[409] which classifies cybercrimes as a tier 1 danger, with a high impact and high probability of occurrence.[410]

22. Kenya

A. National cyber threat landscape

The Communication Authority's first quarter report for 2018/19[411] shows the National Cyber Security Centre (NCC) detected 3.82 million cyber threats, a rise from the 3.46 million reported from the last quarter. In the period between 2018 and 2019, the NCC detected 51.9 million threats, more than double the 22.1 million in 2017–2018.[412] Between October and December 2019, the National Kenya Computer Incident Response Team – Coordination Centre (National KE-CIRT/CC) detected 37.1 million cyber threat events as compared to 25.2 million cyber threat events detected within July–September 2019.[413] By January 2020, the Communications Authority of Kenya (CA)[414] reported that 'cyber threats had increased by over 10 per cent in the first quarter of 2019'.[415] According to the National Cyber Security Index (NCSI),[416] as of January 2023 Kenya ranked: 80th on the NCSI with a score of 41.56; 51st on the Global Cybersecurity Index; 138th on the ICT Development Index; and 84th on the Networked Readiness Index.

B. National cybercrime legislation and related laws

- Kenya Information and Communication Act (KICA) 1998[417]
- Kenya Information and Communications (Amendment) Act 2019[418]
- The Computer Misuse and Cybercrimes Act 2018[419]

405 Jamaica Constabulary Force, Home, available at: https://jcf.gov.jm/, https://jcf.gov.jm/ (accessed 31 January 2023).
406 Director of Public Prosecution, available at: https://dpp.gov.jm/ (accessed 17 January 2023).
407 Major Organised Crime and Anti-Corruption Agency, 'Cyber Crime', available at: www.moca.gov.jm/cyber-crime (accessed 26 January 2023).
408 Vision 2030, Home, available at: www.vision2030.gov.jm/ (accessed 31 January 2023).
409 Government of Jamaica A New Approach: National Security Policy for Jamaica (2014) https://cabinet.gov.jm/wp-content/uploads/2017/05/NATSEC-March-25-2014-1-1.pdf.
410 Ibid, p10.
411 Communications Authority of Kenya (2019), *Cybersecurity Sector Statistics Report Q1-2018-2019*, available at: https://ca.go.ke/wp-content/uploads/2018/12/Sector-Statistics-Report-Q1-2018-2019.pdf (accessed 5 January 2023).
412 UNCTAD, 'Data Protection and Privacy Legislation Worldwide', available at: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide (accessed 6 January 2023).
413 Communications Authority of Kenya (2020), *Cybersecurity Sector Statistics Report Q2-2019-2020*, available at: https://ca.go.ke/wp-content/uploads/2020/03/Cybersecurity-Sector-Statistics-Report-Q2-2019-2020.pdf (accessed 4 January 2023).
414 Communications Authority of Kenya, available at: www.ca.go.ke/ (accessed 6 January 2023).
415 Communications Authority of Kenya, Annual Reports, available at: www.ca.go.ke/downloads/publications/annual-reports/ (accessed 6 January 2023).
416 NCSI: Kenya, available at: https://ncsi.ega.ee/country/ke/ (accessed 14 January 2023).
417 Kenya Information and Communication Act, available at: www.ca.go.ke/wp-content/uploads/2021/02/Kenya-Information-and-Communication-Act-1998.pdf (accessed 4 January 2023).
418 Kenya Information and Communications (Amendment) Act <http://kenyalaw.org/kl/fileadmin/pdfdownloads/bills/2019/TheKenyaInformationandCommunication__Amendment_Bill_2019_NA_Bills_No._61.pdf (accessed 4 January 2023).
419 Computer Misuse and Cybercrimes Act, available at: http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/ComputerMisuseandCybercrimesActNo5of2018.pdf (accessed 4 January 2023).

- Kenya Information and Communications (Consumer Protection) Regulations 2010[420]
- Data Protection Act 2019[421]
- Guidelines on Cybersecurity for Payment Service Providers 2019[422]

C. Scope/application of laws

- The Kenya Information and Communications Act seeks to facilitate the development of the ICT sector, while providing for the regulation of electronic transactions and electronic commerce.[423] It provides for cybercrimes such as unauthorised access to computer data, access with intent to commit offences, unauthorised access to and interception of a computer service, unauthorised modification of computer material, unlawful possession of devices and data, electronic fraud, tampering with computer source documents, publishing of obscene information in electronic form, publication for fraudulent purpose, and unauthorised access to protected systems. It was amended in 2019[424] and provides for electronic transactions and cybersecurity.
- The Computer Misuse and Cybercrimes Act provides for offences relating to computer systems. It also makes provisions to ensure timely and effective detection, prohibition, prevention, response, investigation and prosecution of computer and cybercrimes, and other connected purposes. Part III of the Act makes provision for offences such as interference or unauthorised access of a computer system, cyber espionage, cyber harassment, cybersquatting, phishing, cyber terrorism and child pornography.[425]
- The Kenya Information and Communications (Consumer Protection) Regulations protect consumer rights on ICT services and products, while also recognising consumer obligations. The Regulation further sets out security measures required from licensed telecommunication service providers in the provision of their services.[426]
- The Data Protection Act provides for the regulation of the processing of personal data, the rights of data subjects, and the obligations of data controllers and processors. It prescribes the obligations of data controllers and data processors in the collection of personal data and the responsibility to ensure security measures are in place for the protection of personal data against unlawful destruction, loss, alteration and transfer.[427]
- The Guidelines on Cybersecurity for Payment Service Providers (PSPs) were passed to set out the minimum requirements for PSPs in mitigating cyber risk. Their purpose is to create a safer and more secure cyberspace, and establish a co-ordinated approach to preventing and combatting cybercrime.[428]

---

420 Kenya Information and Communications (Consumer Protection) Regulations, available at: www.ca.go.ke/wp-content/uploads/2020/09/Kenya-Information-and-Communications-Consumer-Protection-Regulations-2010-Draft-Consumer-Protection-Guidelines-8-Sep-2020.pdf (accessed 5 January 2023).

421 Data Protection Act, available at: http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf (accessed 4 January 2023).

422 CBK, Cybersecurity Guideline for Payment Service Providers, available at: www.centralbank.go.ke/2019/07/05/cybersecurity-guideline-for-payment-service-providers/ (accessed 6 January 2023).

423 Kenya Information and Communication Act, available at: www.ca.go.ke/wp-content/uploads/2021/02/Kenya-Information-and-Communication-Act-1998.pdf (accessed 4 January 2023).

424 Kenya Information and Communications (Amendment) Act, available at: http://kenyalaw.org/kl/fileadmin/pdfdownloads/bills/2019/TheKenyaInformationandCommunication__Amendment_Bill_2019_NA_Bills_No._61.pdf (accessed 4 January 2023).

425 Computer Misuse and Cybercrimes Act, available at: http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/ComputerMisuseandCybercrimesActNo5of2018.pdf (accessed 4 January 2023).

426 Kenya Information and Communications (Consumer Protection) Regulations, available at: www.ca.go.ke/wp-content/uploads/2020/09/Kenya-Information-and-Communications-Consumer-Protection-Regulations-2010-Draft-Consumer-Protection-Guidelines-8-Sep-2020.pdf (accessed 5 January 2023).

427 Data Protection Act, available at: http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf (accessed 4 January 2023).

428 CBK, Cybersecurity Guideline for Payment Service Providers, available at: www.centralbank.go.ke/2019/07/05/cybersecurity-guideline-for-payment-service-providers/ (accessed 6 January 2023).

D. Sanctions/penalties for cyber-related crimes

- KICA provides for cyber-related crimes in sections 83U to 84F[429] and prescribes penalties ranging from a monetary fine of 200,000 Kenyan shillings to one million (1,000,000) Kenyan shillings; or terms of imprisonment between two (2) to five (5) years; or both a monetary penalty and terms of imprisonment.
- The Computer Misuse and Cybercrimes Act prescribes criminal sanctions ranging from a fine not exceeding 3 million to 25 million shillings, or to imprisonment for a term not exceeding 3 to 25 years as the case may be, or to both a fine and imprisonment. It sets out the penalty for cyber espionage which causes the death of another, as life imprisonment.

E. National computer emergency response team (CERT)/computer security incident response team (CSIRT)

The National Kenya Computer Incident Response Team – Coordination Centre (National KE-CIRT/CC)[430] has the mandate to co-ordinate responses, manage cybersecurity incidents nationally, and collaborate with relevant actors locally, regionally and internationally.

F. National cybersecurity strategy

The National Cyber Security Strategy 2022–2027 was launched in 2022 to serve as a roadmap to address challenges and threats in the cyber domain.[431] The strategy[432] was developed based on six pillars: cybersecurity governance; cybersecurity policies and laws, regulations and standards; critical information infrastructures protection (CIIP); cybersecurity capability and capacity building; cyber risks and cybercrimes management; and co-operation and collaboration.

G. Initiatives to combat cybercrime

- Kenya is one of the 195 INTERPOL [433] member countries.[434]
- The launch of the Computer and Cyber Crimes Co-ordination Committee[435] (NCCCC) in 2021. Kenya also has the National Cyber Computer Center, which implements the decisions of the committee with respect to enshrining cybersecurity.
- The development of a National Cybersecurity Strategy[436] (in 2014 and 2022), which entrenches principles towards safeguarding the country's cyberspace, and building a secure cybercommunity.
- Establishment of the Kenya Computer Incident Response Team and Co-ordination Centre[437] (KE-CIRT/CC) to co-ordinate cyber responses and manage cybersecurity incidents.
- Establishment of the National Computer and Cybercrimes Coordination Committee.

---

429 'Unauthorized access to computer data, access with intent to commit offences, unauthorized access to and interception of computer service, unauthorized modification of computer material, unlawful possession of devices and data, electronic fraud, tampering with computer source documents, publishing of obscene information in electronic form, publication for fraudulent purpose, and unauthorized access to protected systems.'

430 KE-CIRT – Communications Authority of Kenya, available at: https://ke-cirt.go.ke/ (accessed 6 January 2023).

431 Available at: https://nc4.go.ke/national-cybersecurity-strategy-2022-2027/

432 Kenya Cybersecurity Strategy, available at: https://ict.go.ke/wp-content/uploads/2022/10/KENYA-CYBERSECURITY-STRATEGY-2022.pdf (accessed 4 January 2023).

433 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).

434 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).

435 NC4 Secretariat – NC3, available at: https://nc3.go.ke/nc4-secretariat / (accessed 7 January 2023).

436 Kenya Cybersecurity Strategy, available at: https://ict.go.ke/wp-content/uploads/2022/10/KENYA-CYBERSECURITY-STRATEGY-2022.pdf (accessed 4 January 2023).

437 KE-CIRT – Communications Authority of Kenya, available at: https://ke-cirt.go.ke/ (accessed 6 January 2023).

- The government has also developed initiatives that allow for safeguarding critical information infrastructures, such as the National Broadband Strategy 2018,[438] the National ICT Policy Guidelines 2020,[439] a National Digital Master Plan 2022,[440] and establishment of the National Digital Forensics Laboratory.[441]

23. Kiribati

A. National cyber threat landscape
Exact statistics and data on cybercrime are not readily available on Kiribati; however, according to the National Cyber Security Index (NCSI), Kiribati ranked 159th on the NCSI with a score of 5.6.[442]

B. National cybercrime legislation and related laws
- Telecommunications Act[443]

C. Scope/application of laws
- Part XIV of the Telecommunications Act provides for computer misuse and offences such as unauthorised access to data or a program on a computer, unauthorised access to computer material,[444] unauthorised modification of computer material, unauthorised use or interception of a computer service, and child pornography.[445]

D. Sanctions/penalties for cyber-related crimes
- The Telecommunications Act prescribes liability for offences against computer data and systems to range from a fine of $2,000 to $50,000 Australian dollars to imprisonment from one to ten years, or to both fine and imprisonment. The distribution and exhibition of obscene matter attracts a fine not exceeding $1,000 and imprisonment for a term not exceeding two years or both.[446]

E. National computer emergency response team (CERT)/computer security incident response team (CSIRT)
There is no record of a Kiribati national CERT.

F. National cybersecurity strategy
The objectives of the Kiribati National Cybersecurity Strategy 2020[447] include pursuit of economic growth through ICT and proper protection for all Kiribati citizens against cyber threats.[448] It also recognises the importance of international co-operation in addressing cyberthreats and attacks. The strategy has been developed by the Ministry of Information, Communications, Transport and Tourism Development, with technical assistance from the ITU.

G. Initiatives to combat cybercrime
- Kiribati is one of the 195 INTERPOL [449] member countries.[450]

438 National Broadband Strategy, available at: www.ca.go.ke/wp-content/uploads/2018/02/National-Broadband-Strategy.pdf (accessed 5 January 2023).
439 Communications Authority of Kenya (2020), National ICT Policy Guidelines 2020, available at: www.ca.go.ke/document/national-ict-policy-guidelines-2020-2/ (accessed 7 January 2023).
440 National Digital Master Plan 2022, available at: https://repository.kippra.or.ke/handle/123456789/3580 (accessed 4 January 2023).
441 National Digital Forensics Laboratory, available at: www.cid.go.ke/index.php/sections/forensic-sections/cyber-crime.html (accessed 4 January 2023).
442 NCSI: Kiribati, available at: https://ncsi.ega.ee/country/ki/
443 Telecommunications Act, available at: https://kiribati.tradeportal.org/media/ca2012176.pdf (accessed 15 January 2023).
444 Telecommunications Act, section 107, available at: https://kiribati.tradeportal.org/media/ca2012176.pdf (accessed 15 January 2023).
445 Ibid, section 114.
446 Ibid, section 113.
447 National Cybersecurity Strategy, available at: www.mict.gov.ki/sites/default/files/National%20Cybersecurity%20Policy_0.pdf (accessed 24 January 2023).
448 Ibid.
449 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
450 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).

- The formulation of the Kiribati Vision 20 (KV2016–2036).[451] This contains the country's 20-year vision, with peace and security as a pillar. The government intends to 'prioritise national internet security as a pillar for a secure, peaceful and prosperous Kiribati'.
- The establishment of the Kiribati Development Plan 2020–2023.[452] Part of the itemised objectives of the plan are ensuring cyber safety and regulating harmful digital communications.
- The implementation of the National ICT Policy 2019,[453] where the government reiterated cybersecurity as an important component while promising a 'robust and reliable ICT environment'.

24. Lesotho

A. National cyber threat landscape

Exact statistics and data on cybercrime are not available on Lesotho. Lesotho's parliament approved the Computer Crime and Cyber Security Bill in 2022.

B. National cybercrime legislation and related laws

- Computer Crime and Cyber Security Bill[454]
- Communication Act 2012[455]

C. Scope/application of laws

- The Computer Crime Bill 'criminalises computers and network related crime; provides for investigation and collection of evidence for computer and network related crime; and provides for the admission of electronic evidence for such offences'. In general, it provides a legal framework for the criminalisation of computer- and network-related offences. Part II of the Act provides for offences such as illegal access, illegal interception, illegal data interface, espionage, illegal system interference, computer-related forgery, computer-related fraud, cyber terrorism, cyber extortion, child pornography, identity-related crimes and harassment utilising means of electronic communication.
- The Communication Act provides for the regulation of the telecommunications, broadcasting and postal sectors, and prescribes offences such as the unauthorised interception or tracing of communication operations.

D. Sanctions/penalties for cyber-related crimes

- Part II of the Computer Crime and Cyber Bill prescribes penalties to the offences stated thereto, to the range of imprisonment for a period between one and seven years, or a fine between 5,000 and 90,000 maloti (M), or both fine and imprisonment.
- Section 44 of the Lesotho Communication Act prescribes the penalty of imprisonment not exceeding a term of five years, or a fine not exceeding M50,000, or both a fine and imprisonment.

E. National computer emergency response team (CERT)/computer security incident response team (CSIRT)

There is no record of a Lesotho national CERT.

---

451 Kiribati Vision, available at: www.mfed.gov.ki/sites/default/files/KIRIBATI%2020-YEAR%20VISION%202016-2036%20.pdf (accessed 26 January 2023).

452 Kiribati Development Plan, available at: https://policy.asiapacificenergy.org/sites/default/files/Kiribati%20Development%20Plan%202020-2023.pdf (accessed 15 January 2023).

453 National ICT Policy, available at: www.mict.gov.ki/sites/default/files/National%20ICT%20Policy.pdf (accessed 13 January 2023).

454 Computer Crime and Cybercrime Bill, available at: https://ictpolicyafrica.org/es/document/7hwpifnqr6l (accessed 14 January 2023).

455 Lesotho Communication Act 2012, available at: https://ictpolicyafrica.org/pt/document/z8vyhu6uj2 (accessed 13 January 2023).

F. National cybersecurity strategy
There is no record of a Lesotho national cyber security strategy.

G. Initiatives to combat cybercrime
Lesotho is one of the 195 INTERPOL [456] member countries.[457]

25. Malawi

A. National cyber threat landscape
According to the National Cyber Security Index (NCSI),[458] as of January 2023 Malawi ranked: 105th on the NCSI with a score of 22.27; 97th on the Global Cybersecurity Index; 167th on the ICT Development Index; and 119th on the Networked Readiness Index.

B. National cybercrime legislation and related laws

- Electronic Transactions and Cyber Security Act 2016[459]

C. Scope/application of laws

- The Electronic Transactions and Cyber Security Act makes provision for electronic transactions; for the establishment and functions of the Malawi Computer Emergency Response Team (MCERT); criminalises offences related to computer systems and information communication technologies; provides for investigation, collection and use of electronic evidence; and for matters connected therewith and incidental thereto.

D. Sanctions/penalties for cyber-related crimes

- The Electronic Transactions and Cyber Security Act 2016 prescribes for some cyber-related offences. Section 87(3) of the Act punishes any person who 'intercepts any data without authority or permission to do so'. Section 87(4) of the Act punishes any person who 'interferes with data in a way which causes such data to be modified, destroyed or otherwise rendered ineffective'. It also provides for offences such as unauthorised access, interception or interference with data, child pornography, cyber harassment, cyber stalking, and spamming. It then prescribes a fine of 1,000,000 to 10,000,000 Malawi kwacha and imprisonment from 12 months to 15 years.

E. National computer emergency response team (CERT)/computer security incident response team (CSIRT)
Malawi Computer Emergency Response Team (MCERT)[460] was established pursuant to section 6 of the Electronic Transaction and Cyber Security Act 2016 of the Laws of Malawi for national co-ordination and response to cybersecurity threats in the country.

F. National cybersecurity strategy
The five-year Malawi National Cybersecurity Strategy[461] was approved by the Government of Malawi in 2019.

G. Initiatives to combat cybercrime

- Malawi is one of the 195 INTERPOL [462] member countries.[463]

456 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
457 Interpol member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).
458 NCSI: Malawi, available at: https://ncsi.ega.ee/country/mw/ (accessed 14 January 2023).
459 MACRA, Electronic Transaction and Cyber Security Act 2016, available at: https://macra.mw/download/electronic-transaction-and-cyber-security-act-2016/ (accessed 14 January 2023).
460 Malawi's Computer Emergency Response Team (MwCERT), available at: www.mwcert.mw/ (accessed 14 January 2023).
461 Malawi National Cybersecurity Strategy, available at: www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/00019_07_Malawi%20national-cybersecurity-strategy.pdf (accessed 13 January 2023).
462 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
463 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).

- Creation of the Malawi Communications Regulatory Authority (MACRA).[464] This was established pursuant to section 3 of the Communications Act.[465] It 'regulates and monitors the provision of communications services; and ensures that, as far as it is practicable, reliable and affordable communications services are provided throughout Malawi'.[466] The Department of E-Government within the Ministry of Information also exercise cybersecurity authority.
- Establishment of Malawi's Computer Emergency Response Team, to ensure national co-ordination and response to cybersecurity threats in the country.
- Appointment of cyber inspectors to oversee the cyber landscape in the country.
- The development of the Malawi ICT Policy,[467] which has among its policy statements the development of national security, wherein the 'Government shall enhance the capacity of security agencies to be up to date with developments in the ICT sector, including cyber crimes'.[468]

26. Malaysia

A. National cyber threat landscape
According to the National Cyber Security Index (NCSI),[469] as of January 2023 Malaysia ranked: 20th out of 161 countries on the NCSI with a score of 79.22; 5th out of 194 countries on the Global Cybersecurity Index; 63rd on the ICT Development Index; and 36th on the Networked Readiness Index.It was reported that, 'between 2017 and 2021, the total amount lost to cybercrime in Malaysia was estimated at RM2.23 billion ($490 million). From January to July 2022, there were 11,367 reported cases of cybercrime, with the rate of crime increasing 61% from 2016 to 2022'.[470]

B. National cybercrime legislation and related laws
- Computer Crimes Act 1997[471]

C. Scope/application of laws
- The Computer Crimes Act provides for offences relating to the misuse of computers. Part II of the Act provides for offences such as unauthorised access to computer material, unauthorised access with intent to commit or facilitate commission of further offence, and unauthorised modification of the contents of a computer.

D. Sanctions/penalties for cyber – related crimes
- The Computer Crimes Act prescribes penalty of a fine between 50,000 ringgit (RM) to 150,000 ringgit or imprisonment for a term between five and ten years, or to both.

E. National computer emergency response team (CERT)/computer security incident response team (CSIRT)
Malaysia Computer Emergency Response Team (MyCERT)[472] was formed in 1997 and provides a timely response to computer security and related matters in Malaysia.[473]

464 Malawi Communications Regulatory Authority (MACRA), available at: https://macra.mw/ (accessed 23 January 2023).
465 Communications Act, available at: https://macra.mw/storage/2014/07/Communications-Act-2016.pdf (accessed 24 January 2023).
466 MACRA, Home, available at: https://macra.mw/ (accessed 29 January 2023).
467 Malawi ICT Policy, available at: https://comesabusinesscouncil.org/wp-content/uploads/2020/04/6-Malawi-ICT-Policy-2013-1.pdf (accessed 28 January 2023).
468 Ibid.
469 NCSI: Malaysia, available at: https://ncsi.ega.ee/country/my/ (accessed 17 January 2023).
470 'The Latest 2023 Cyber Crime Statistics', available at: https://aag-it.com/the-latest-cyber-crime-statistics/ (accessed 9 January 2023).
471 Computer Crimes Act 1997, available at: http://www.commonlii.org/my/legis/consol_act/cca1997185/ (accessed 18 January 2023).
472 MyCERT, Home, available at: www.mycert.org.my/ (accessed 26 January 2023).
473 Cyber Security Malaysia, available at: www.cybersecurity.my/en/our_services/mycert/main/detail/2328/index.html (accessed 26 January 2023).

F. National cybersecurity strategy

The Malaysia Cybersecurity Strategy (MCSS) 2020–2024[474] aims to provide trust in the country's cyber environment, and support the government agenda in the digital economy. The strategy replaces the country's National Cybersecurity Policy (NCSP),[475] which was put in place as an acknowledgement of the cyber threats endangering the country's e-sovereignty.

G. Initiatives to combat cybercrime

- Malaysia is one of the 195 INTERPOL [476] member countries.[477]
- Establishment of governmental entities that, among other functions, develop frameworks and offer services to combat cyber threats. These include the Ministry of Science, Technology, and Innovation (MOSTI), the Malaysian Communications and Multimedia Commissions (MCMCs)[478] and Cyber Security Malaysia (CSM),[479] to provide technological security services and preserve policies.
- Adoption of computer forensic investigation using digital forensic tools to aid the detection of cyber offenders, investigation of cybercrimes and to solve incidences of cybercrime in the country. Forensic laboratories include the Cheras Computer Forensic Laboratory, the Cybersecurity Office and the Military Office.
- The launch of the Malaysia Cybersecurity Cyber Threat Research Centre[480] on 2 December 2009. The centre 'operates a distributed research network for analysing malware and computer security threats'. It also collaborates with other institutions in analysing and sharing threat research information.
- Facilitation of cyber awareness programmes such as 'CyberSafe',[481] where online security issues to ensure a safe and secured cyber landscape are discussed with Malaysians.
- Institution of an Incident Report Center to allow online reporting of cyber incidents. The public can escalate incidents using the Cyber999 Center.[482]
- Establishment of the Malaysia National Cyber Coordination and Command Centre[483] (NC4) to deal with threats arising in the country's cyber space.
- Setting up of the National Cyber Crisis Exercise (X-Maya) to test the 'effectiveness of procedures set up under the Malaysia National Cyber Crisis Management Plan (NCCMP)[484] and assess the readiness and preparedness of critical national infrastructure agencies against cyberattacks'.[485]

474 Cybersecurity Strategy 2020–2024, available at: https://asset.mkn.gov.my/web/wp-content/uploads/sites/3/2019/08/MalaysiaCyberSecurityStrategy2020-2024Compressed.pdf (accessed 27 January 2023).
475 Cyber Security Malaysia, available at: www.cybersecurity.my/en/knowledge_banks/journal_conference/main/detail/2397/index.html (accessed 1 February 2023).
476 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
477 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).
478 Malaysian Communications and Multimedia Commissions, available at: www.mcmc.gov.my/en/home (accessed 23 January 2023).
479 Cyber Security Malaysia, available at: www.cybersecurity.my/ (accessed 31 January 2023).
480 Cyber Security Malaysia, available at: www.cybersecurity.my/en/our_services/research/main/detail/2331/index.html (accessed 31 January 2023).
481 CyberSAFE, available at: www.cybersafe.my/en/ (accessed 31 January 2023).
482 Cyber999, available at: www.cybersafe.my/cyber999.html (accessed 31 January 2023).
483 National Cyber Coordination and Command Centre (NC4) – Malaysia, available at: www.cybersecurityintelligence.com/national-cyber-coordination-and-command-centre-nc4-malaysia-7738.html (accessed 1 February 2023)
484 NACSA, National Cyber Crisis Management Plan, available at: www.nacsa.gov.my/nccmp.php (accessed 1 February 2023)
485 Cybersecurity Strategy 2020–2024, available at: https://asset.mkn.gov.my/web/wp-content/uploads/sites/3/2019/08/MalaysiaCyberSecurityStrategy2020-2024Compressed.pdf (accessed 27 January 2023).

27. Maldives

A. National cyber threat landscape

Exact statistics and data on the cybercrime threat landscape are not available for Maldives on the National Cyber Security Index. Maldives does not have any officially recognised national legislation pertaining particularly to cybercrime.

B. National cybercrime legislation and related laws

- Penal Code (Law No6/2014)[486]
- Criminal Procedure Code (Act No. 12/2016)[487]
- Maldives Act on Mutual Legal Assistance in Criminal Matters (Act No. 2/2015)[488]

C. Scope/application of laws

The penal code of Maldives prescribes criminal offenses, requirements of offense liability, offence elements, penalties for offences, offence grades and implications, defences against offences, sentencing guidelines and punishments, along with all the procedures relating to determining of penalties. Changes have been drafted for the law, to empower authorities to stop and take action against crimes that involve electronic evidence, and establish policies for investigation and prosecution of cybercrimes.[489]

D. National computer emergency response team (CERT)/computer security incident response team (CSIRT)

Maldives does not currently have an officially recognised national CERT/CSIRT.

E. National cybersecurity strategy

Maldives does not have any officially recognised national cybersecurity strategy for implementing internationally recognised cybersecurity standards. However, the Communication Authority of Maldives is the officially recognised agency responsible for implementing the country's cybersecurity-related strategies, policies and roadmap.

F. Initiatives to combat cybercrime

- Maldives is one of the 195 INTERPOL [490] member countries.[491]
- Review of extant laws in the country to make provisions for cybercrime. It was reported on 27 November 2022 that the Attorney General's Office (AGO) had drafted legislative changes to the Penal Code, Criminal Procedure Code and the Act on Mutual Legal Assistance in Criminal Matters, to criminalise cybercrime and tackle the increase in cybercrime in Maldives.[492]
- Establishment of the 'Cyber Safe Maldives' initiative along with Cyber Awareness Month, as part of the nation's 'cybersecurity efforts' and the organisation of different programmes that include 'a total of 28 activities, including seven training programmes, three panel discussions, and 16 awareness sessions' to inform and encourage online safety among the people.[493]

---

486 Maldives Penal Code, available at: www.law.upenn.edu/live/files/4203-maldives-penal-code-2014 (accessed 18 January 2023).

487 Maldives Criminal Procedure Code (Act No. 12/2016), available at: www.ilo.org/dyn/natlex/natlex4.detail?p_lang=en&p_isn=106006&p_country=MDV&p_count=20&p_classification=01.04&p_classcount=4 (accessed 23 January 2023).

488 Mutual Legal Assistance in Criminal Matters Act (Act No. 2/2015).

489 SunOnline International, 'AGO Drafts Legislative Changes to Tackle Rise in Cybercrime', available at: https://en.sun.mv/79332 (accessed 23 January 2023).

490 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).

491 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).

492 SunOnline International, AGO Drafts Legislative Changes to Tackle Rise in Cybercrime, available at: https://en.sun.mv/79332 (accessed 23 January 2023).

493 The President's Office, 'Cyber Safe Maldives will be the basis for safe internet and technology use in Maldives, says Vice President', available at: https://presidency.gov.mv/Press/Article/27369 (accessed 26 January 2023).

28. Malta

A. National cyber threat landscape

According to the National Cyber Security Index (NCSI),[494] as of January 2023 Malta ranked: 73rd out of 161 countries on the NCSI with a score of 50.65; 49th out of 194 countries on the Global Cybersecurity Index; 24th on the ICT Development Index; and 31st on the Networked Readiness Index.

B. National cybercrime legislation and related laws

- Criminal Code of Malta (Cap. 9)[495]

C. Scope/application of laws

- The Criminal Code amends and consolidates the Penal Laws and the Laws of Criminal Procedure in Malta. Section 337 of the Act provides for offences that constitute misuse of computer systems or data such as unlawful access, interference and interception, or use of, information.

D. Sanctions/penalties for cyber-related crimes

- Section 337F of the Criminal Code provides that any person who contravenes the provisions of the Act on misuse of computer systems, 'shall be guilty of an offence and shall be liable on conviction to a fine (multa) not exceeding twenty-three thousand and two hundred and ninety-three euro and seventy-three cents (23,293.73) or to imprisonment for a term not exceeding four years, or to both such fine and imprisonment'. It further provides for an increased fine for a second or subsequent offences, and imprisonment for a term from 12 months to 10 years in aggravating circumstances.

E. National computer emergency response team (CERT)/computer security incident response team (CSIRT)

The Government Computer Security Incident Response Team[496] is tasked with 'detecting, preventing, protecting and responding to potential cyberattacks towards the Maltese Government'.[497]

F. National cybersecurity strategy

The National Cyber Security Strategy proposes six goals, that is: 'establish a governance framework; combat cybercrime; strengthen national cyber defence; secure cyberspace; cybersecurity awareness and education; and national and international co-operation'. A National Cybersecurity Strategy 2023–2026 has recently been articulated to build on the previous strategy, allowing for evolving challenges and realities.

G. Initiatives to combat cybercrime

- Malta signed the Convention on Cybercrime (ETS No. 185)[498] on 17 January 2002 and ratified it on 12 April 2012. It came into force in the country on 1 August 2012.[499]
- Another initiative to combat cybercrime in the country is being party to the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224)[500] of 12 May 2022. The protocol 'provides

494 NCSI: Malta, available at: https://ncsi.ega.ee/country/mt/ (accessed 17 January 2023).
495 Criminal Code of Malta, available at: https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=NIM:202100290 (accessed 13 January 2023).
496 Government Computer Security Incident Response Team (MITA), available at: https://mita.gov.mt/government-computer-security-incident-response-team/ (accessed 26 January 2023).
497 Ibid.
498 Council of Europe, 'The Budapest Convention (ETS No. 185) and is Protocols', available at: www.coe.int/en/web/cybercrime/the-budapest-convention (accessed 26 January 2023).
499 Council of Europe, 'Complete list of Council of Europe's treaties', Treaty Office, available at: www.coe.int/en/web/conventions/full-list (accessed 25 January 2023).
500 Council of Europe, 'Enhanced co-operation and disclosure of electronic evidence: 22 countries open the way by signing the Second Additional Protocol to the Cybercrime Convention', available at: www.coe.int/en/web/cybercrime/second-additional-protocol/-/asset_publisher/isHU0Xq21Ihu/content/opening-coecyber2ap (accessed 26 January 2023).

tools for enhanced co-operation and disclosure of electronic evidence – such as direct co-operation with service providers and registrars, effective means to obtain subscriber information and traffic data, immediate co-operation in emergencies or joint investigations – that are subject to a system of human rights and rule of law, including data protection safeguards'.[501]

- Malta is one of the 195 INTERPOL [502] member countries.[503]
- Implementation of 'Digital Malta', the national digital strategy[504] for the country. The strategy puts forward 'guiding principles and actions for ICT to be used for socio-economic development. It sets out how ICT can make a difference in areas such as the economy and how it can be used for national development, to empower citizens and transform government'.[505]
- Implementation of the country's National Cyber Security Strategies.[506] This intends to inculcate an awareness of cybersecurity, its extent and its implications to the citizenry. It proposes six goals, that is: 'establish a governance framework; combat cybercrime; strengthen national cyber defence; secure cyberspace; cybersecurity awareness and education; and national and international co-operation'.
- Implementation of the National E-Security Strategy Policy,[507] which aims among others, to ensure the enforcement and prosecution of cybercrime in the country.
- The establishment of the Cybersecurity National Coordination Centre (NCC). [508]
- Adoption of standards and instruments, such as the adoption of ISO 27001[509] by organisations and governmental bodies in Malta to govern their information security management operations;[510] and the Government of Malta ICT Policies, Malta Directives and Standards (GMICT) Information Security Policy Framework of 10 December 2017.[511]
- Incentivising organisations by, for instance, giving tax credit to an organisation for capital investments made in relation to its information technology infrastructure. This encourages organisations to implement more cybersecurity and IT infrastructure.
- Establishment of a specialised Cyber Crime Unit[512] in the Maltese police force. Established in 2003, the major responsibility of the unit is to 'provide technical assistance in the detection, investigation and prosecution of crime wherein the computer is the target or the means used'.[513] Police officers in the unit are skilled in detecting and investigating cybercrime.

501 Ibid.
502 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
503 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).
504 'Digital Malta – the National Digital Strategy for the period 2014 till 2020', available at: https://digitalmalta.org.mt/en/Documents/Digital%20Malta%202014%20-%202020.pdf (accessed 28 January 2023).
505 Ibid.
506 National Cyber Security Strategies, available at: www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSSGreenPaper.pdf (accessed 27 January 2023).
507 Malta Communications Authority eSecurity: A Strategic Direction, available at: www.mca.org.mt/sites/default/files/consultations/esecurity-cons-paper-to-publish.pdf (accessed 27 January 2023).
508 Cybersecurity National Coordination Centre, available at: https://ncc-mita.gov.mt/
509 ISO, ISO/IEC 27001 and Related Standards — Information Security Management, available at: www.iso.org/isoiec-27001-information-security.html (accessed 31 January 2023).
510 Zammit, WP-R and Finkel, O (2019), 'Cybersecurity in Malta' *Lexology*, 25 February, available at: www.lexology.com/library/detail.aspx?g=39f7af30-dcee-423e-b2af-957b4fd94b16 (accessed 26 January 2023).
511 MITA, GMICT Policies, available at: https://mita.gov.mt/portfolio/ict-policy-and-strategy/gmict-policies/ (accessed 31 January 2023).
512 Cyber Crime Unit, available at: https://pulizija.gov.mt/en/police-force/police-sections/Pages/Cyber-Crime-Unit.aspx (accessed 26 January 2023).
513 Ibid.

- International co-operation and continuous upskilling of personnel through initiatives of agencies such as I INTERPOL [514] and Europol.[515]
- Participation in the 'CSIRTs network and in the European Cooperation Group to ensure the effective, efficient and secure co-operation at the European level'.[516]

29. Mauritius

A. National cyber threat landscape
According to the National Cyber Security Index (NCSI),[517] as of January 2023 Mauritius ranked: 77th on the NCSI with a score of 44.16; 17th on the Global Cybersecurity Index; 72nd on the ICT Development Index; and 71st on the Networked Readiness Index.

B. National cybercrime legislation and related laws –
- Computer Misuse and Cyber Crimes Act 2003[518]
- The Information and Communication Technologies Act 2001[519]
- Data Protection Act 2017[520]
- Electronic Transactions Act (ETA) 2000[521]
- Child Protection Act 1994[522]

C. Scope/application of laws
- The Computer Misuse and Cyber Crimes Act provides for criminal offences relating to cybercrime and the related rules for investigations and procedures. Part II of the Act provides for offences such as unauthorised access to computer data, access with intent to commit offences, unauthorised access to and interception of a computer service, unauthorised modification of computer material, damaging or denying access to a computer system, unauthorised disclosure of a password, unlawful possession of devices and data, and electronic fraud.
- The ICT Act establishes the ICT Authority, the ICT Advisory Council and the ICT Appeal Tribunal, and provides for the regulation and democratisation of information and communication technologies and related matters. Section 46 of the ICT Act deals with criminal offences such as: harming the functioning of an information and communication service, including telecommunication service; forgery; using an information and communication service, including telecommunication service, to impersonate; dishonestly obtaining or making use of an information and communication service, including telecommunication service; intercepting, or authorising another person to intercept, a message passing over a network.
- The Electronic Transactions Act 2000 provides for an appropriate legal framework to facilitate electronic transactions and communications, by regulating electronic records and electronic signatures and the security thereof.

514 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
515 Law Enforcement Cooperation, European Union (Europol), available at: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/europol_en (accessed 30 January 2023).
516 CSIRTMalta, available at: https://maltacip.gov.mt/en/CIP_Structure/Pages/CSIRTMalta.aspx (accessed 26 January 2023).
517 NCSI: Mauritius, available at: https://ncsi.ega.ee/country/mu/ (accessed 14 January 2023).
518 Computer Misuse and Cyber Crimes Act 2003, available at: www.imolin.org/doc/amlid/Maurituis/cyber.pdf (accessed 13 January 2023).
519 Information and Communication Technologies Act 2001, available at: https://en.unesco.org/creativity/sites/creativity/files/qpr/icta_act.pdf (accessed 13 January 2023).
520 Data Protection Act 2017, available at: https://dataprotection.govmu.org/Pages/The%20Law/Data-Protection-Act-2017.aspx (accessed 13 January 2023).
521 Electronic Transaction Act 2000, available at: www.mcci.org/media/36445/electronic-transaction-act-2000.pdf (accessed 14 January 2023).
522 Child Protection Act, available at: www.icta.mu/documents/2021/08/child_protection.pdf (accessed 13 January 2023).

- The Child Protection Act, among other provisions, criminalises child pornography and the illegal use of indecent child photograph in sections 14 and 15.

D. Sanctions/penalties for cyber-related crimes
- The Computer Misuse and Cyber Crimes Act prescribes the penalty, on conviction, to a fine ranging from 50,000 Mauritian rupees (MRs) to MRs200,000 and to penal servitude between 5 and 20 years.
- Section 47 of the ICT Act prescribes the penalties in the Act. It provides, that 'any person who commits an offence under this Act, shall, on conviction, be liable to a fine not exceeding 1,000,000 rupees and to penal servitude for a term not exceeding 10 years'.
- Section 47 of the ETA provides for fines between MRs50,000 to 100,000 and imprisonment ranging from 12 months to five years, for offences committed under the Act.
- The Child Protection Act provides that anyone who commits an offence under sections 14 and 15 shall, on conviction, be liable, where the victim is mentally handicapped, to penal servitude for a term not exceeding 30 years; or in any other case, to a fine not exceeding MRs100,000 and to penal servitude for a term not exceeding 20 years.

E. National computer emergency response team (CERT)/computer security incident response team (CSIRT)
The Mauritian National Computer Security Incident Response Team (CERT-MU) operates under the auspices of National Computer Board to provide information and assistance for implementing proactive measures to address cybersecurity incidents, as well as responding to cyber incidents.

F. National cybersecurity strategy
Mauritius has both a Cybercrime Strategy[523] and a Cybersecurity Strategy.[524]The two policy documents set out the government's approach to combat cybercrime in the country. In combatting cybercrime, the government believes that there is a need to have a 'cybercrime strategy that runs in parallel and deals with the issues pertaining to the investigation and prosecution of criminals, and the role of the criminal justice system, while the cybersecurity strategy focuses on prevention, mitigation and defence of critical national infrastructure assets'.[525] The country already had a Cybersecurity Strategy that ran from 2014 to 2019. The goals of the Cybercrime Strategy include: 'ensuring that law enforcement agencies are able to detect, investigate cybercrime in a more efficient way; providing a more effective legal framework for investigating and prosecuting cybercrime; enhancing the capacity of the judiciary to deal with cybercrime and digital evidence; developing an enhanced intelligence picture of the cybercrime threat facing Mauritius; working with international counterparts to improve co-operation on cybercrime; supporting the industry by responding to the shared problem of cybercrime; and educating the community on the risks of cybercrime'.[526] The Ministry of Technology, Communication and Innovation has been charged with driving cybersecurity policy with the aim of improving overall cybersecurity preparedness.

G. Initiatives to combat cybercrime
- Mauritius, on 15 November 2013, became the first African country to accede to the Convention on Cybercrime ETS No. 185 ('the Budapest Convention'). It came into force in the country on 1 March 2014.[527]

523 Cybercrime Strategy Mauritius, available at: http://cert-mu.govmu.org/English/Documents/Cybercrime%20Strategy/National%20Cybercrime%20Strategy-%20August%202017.pdf (accessed 13 January 2023).
524 Cybersecurity Strategy Mauritius, available at: http://mitci.govmu.org/English/Documents/Final%20National%20Cyber%20Security%20Strategy%20November%202014.pdf (accessed 13 January 2023).
525 Cybercrime Strategy Mauritius, available at: http://cert-mu.govmu.org/English/Documents/Cybercrime%20Strategy/National%20Cybercrime%20Strategy-%20August%202017.pdf (accessed 13 January 2023).
526 Ibid.
527 Council of Europe, 'The Budapest Convention (ETS No. 185) and its Protocols', available at: www.coe.int/en/web/cybercrime/the-budapest-convention (accessed 26 January 2023).

- Mauritius is one of the 195 INTERPOL [528] member countries.[529]
- Inclusion of a Cybercrime Unit in the Office of the Director of Public Prosecutions.[530] The unit is responsible for cyber prosecutions in Mauritius.
- Creation of the Mauritian National Computer Security Incident Response Team (CERT-MU) to ensure timely intervention on cyber incidents in the country.
- Establishment of the Mauritian Cybercrime Online Reporting System (MAUCORS).[531] The system was designed to facilitate cybercrime reporting and develop a better understanding of the cybercrime affecting Mauritian citizens. It 'allows the public to report cybercrimes occurring on social media securely, while providing advice to help in recognising and avoiding common types of cybercrime which take place on social media websites'.[532]
- Implementation of both a Cybercrime Strategy[533] and a Cybersecurity Strategy,[534] which set out the government's approach to combat cybercrime in the country. The government believes there needs to be a 'cybercrime strategy that runs in parallel and deals with the issues pertaining to the investigation and prosecution of criminals, and the role of the criminal justice system, while the cybersecurity strategy focusses on prevention, mitigation and defence of critical national infrastructure assets'.[535]
- The International Telecommunication Union (ITU) Centre of Excellence in the focus area of cybersecurity, which was set up in 2019 by the National Computer Board and which operates under the aegis of the Mauritian Ministry of Information Technology, Communication and Innovation in collaboration with the CERT-MU.[536]
- Mauritius has also ratified the AU Convention on Cyber Security and Personal Data Protection ('the Malabo Convention') 2014.
- The government further engages in capacity building for its law enforcement agents and other security personnel.

30. Mozambique

A. National cyber threat landscape

According to the National Cyber Security Index (NCSI),[537] as of January 2023 Mozambique ranked: 150th on the NCSI with a score of 9.09; 123rd on the Global Cybersecurity Index; 150th on the ICT Development Index; and 125th on the Networked Readiness Index.

B. National cybercrime legislation and related laws

- Law No. 3/2017 on Electronic Transactions
- The Penal Code, Law No. 24/2019[538]

528 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
529 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).
530 The DPP, available at: https://dpp.govmu.org/Pages/About%20Us/The-DPP.aspx (accessed 29 January 2023).
531 The Mauritian Cybercrime Online Reporting System (MAUCORS), available at: https://maucors.govmu.org/maucors/ (accessed 29 January 2023).
532 Ibid.
533 Cybercrime Strategy Mauritius, available at: http://cert-mu.govmu.org/English/Documents/Cybercrime%20Strategy/National%20Cybercrime%20Strategy-%20August%202017.pdf (accessed 13 January 2023).
534 Cybersecurity Strategy Mauritius, available at: http://mitci.govmu.org/English/Documents/Final%20National%20Cyber%20Security%20Strategy%20November%202014.pdf (accessed 13 January 2023).
535 Cybercrime Strategy Mauritius, available at: http://cert-mu.govmu.org/English/Documents/Cybercrime%20Strategy/National%20Cybercrime%20Strategy-%20August%202017.pdf (accessed 13 January 2023).
536 TU Centre of Excellence in Mauritius (Focus area: Cybersecurity), available at: https://cert-mu.govmu.org/Pages/ITU-Centre-of-Excellence-in-Mauritius.aspx
537 NCSI: Mozambique, available at: https://ncsi.ega.ee/country/mz/ (accessed 14 January 2023).
538 Penal Code, available at: https://reformar.co.mz/documentos-diversos/lei-24-2019-lei-de-revisao-do-codigo-penal.pdf (accessed 14 January 2023).

- Law No. 14/2013 on Preventing and Combatting Money Laundering and Financing of Terrorism

C. Scope/application of laws
- The Electronic Transactions Act, approved by Law No. 3/2017 of 9 January 2017, provides a general legal framework for electronic transactions, e-commerce and e-government.[539] Article 67 thereof mentions a range of offences, such as: illegal access to a computer or computer network; illegal interception of private data transmission via a computer or computer network; data interference; intentional interference with computer systems affecting their functioning; and other interference with the functioning of computer systems or computer networks.
- Articles 336 to 339 of the Penal Code provide for computer fraud and related crimes. The Code prescribes a penalty of imprisonment ranging from one to two years and a fine. It further prescribes an increased term of eight years' imprisonment in aggravated circumstances.

D. National computer emergency response team (CERT)/computer security incident response team (CSIRT)
The Mozambique National Computer Emergency Response Team (CERT-MZ).[540]

E. National cybersecurity strategy
The National Cyber Security Strategy of Mozambique:[541] 'aims to create a safer and resilient cyberspace for the Government, private sector, civil society and other institutions'. The key objectives of the strategy include: 'Improve the protection of critical information infrastructure (ICI); strengthen the legal, technical and operational cybersecurity framework; establish a national framework to promote information sharing, co-operation and co-ordination on cyber-security; develop technical capacity for research and innovation in security cybernetics; and creating a national culture of cybersecurity'.[542]

F. Initiatives to combat cybercrime
- Mozambique is one of the 195 INTEROL member countries.[543,544]
- Facilitation of training and workshops for law enforcement agents. For instance, the International Organization for Migration (IOM) conducted a series of criminal investigation trainings and trainings of trainers (ToT)[545] in Maputo on 28 October 2022.
- Continuous efforts by the government to discuss ways of entrenching cybersecurity in the country. An example is one of the meetings held by the Government of Mozambique, through the Ministry of Science and Technology, Higher Education and Technical Professional, and MISA (Media Institute of Southern Africa) Mozambique to explore ways to create safer and more secure use of ICT in the country. The stakeholders

539 Review of the Electronic Transactions Act in Mozambique (1 August 2017), available at: https://lexafrica.com/2017/08/review-of-the-electronic-transactions-act-in-mozambique/ (accessed 15 January 2023).
540 CERT-MZ, available at: http://www.cert.mz/ (accessed 15 January 2023).
541 National Cyber Security Strategy of Mozambique, available at: www.oam.org.mz/wp-content/uploads/2017/06/Draft_National_Cyber_Security_Strategy_Mozambique_PT_GT_24052017FINAL.pdf (accessed 30 January 2023).
542 Ibid.
543 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 30 January 2023).
544 Mozambique, available at: www.interpol.int/en/Who-we-are/Member-countries/Africa/MOZAMBIQUE (accessed 30 January 2023).
545 'IOM and the German cooperation support the Government of Mozambique to improve community safety and strengthen border security in Northern Mozambique', available at: https://mozambique.iom.int/news/iom-and-german-cooperation-support-government-mozambique-improve-community-safety-and-strengthen-border-security-northern-mozambique (accessed 30 January 2023).

also discussed the 'challenges and opportunities that exist in the framework of the establishment of a legislative package on cybersecurity based on citizens' rights and freedoms'.[546]

31. Namibia

A. National cyber threat landscape
According to the National Cyber Security Index (NCSI),[547] as of January 2023 Namibia ranked: 133rd on the NCSI with a score of 15.58; 115th on the Global Cybersecurity Index; 118th on the ICT Development Index; and 109th on the Networked Readiness Index.

B. National cybercrime legislation and related laws
- Electronic Transactions and Cybercrime Act 2016[548]
- Communications Act 8 of 2009[549]
- Electronic Transactions Act (ETA) 2019[550]
- Draft Data Protection Policy

C. Scope/application of laws
- The Electronic Transactions and Cybercrime Act provides a general framework for the promotion of the use of electronic transactions in government services and private contracts; and the legal recognition of electronic transactions; and outlines certain cybercrime offences and the powers for the investigation of the offences. Chapter 8 of the Act provides for cybercrimes such as unauthorised access,[551] unauthorised interference,[552] child pornography,[553] electronic harassment[554] and other offences.[555]
- The ETA 2019 provides for the legal recognition of electronic transactions; the admission of electronic evidence; and provides for consumer protection in electronic commerce.
- The Communications Act provides for the regulation of telecommunications. Part 6 of Chapter V (interception of telecommunications) of the Act was brought into force with effect from 1 January 2023 by GN292/2022[556].

D. Sanctions/penalties for cyber-related crimes
- Liability for cybercrimes committed under Chapter 8 of the Electronic Transactions and Cybercrime Act ranges from a fine not exceeding 10,000 to 1,000,000 Namibia dollars (N$) or to imprisonment for a period not exceeding 2 to 20 years, or to both such fine and such imprisonment.

E. National computer emergency response team (CERT)/computer security incident response team (CSIRT)

---

546 'Government and MISA Mozambique explore synergies for cyber security', available at: www.misa.org.mz/index.php/destaques/noticias/85-government-and-misa-mozambique-explore-synergiesfor-cyber-security (accessed 30 January 2023).
547 NCSI: Namibia, available at: https://ncsi.ega.na/country/mu/ (accessed 14 January 2023).
548 Electronic Transactions and Cybercrime Act 2016, available at: https://mict.gov.na/documents/32978/0/Latest+Copy+of+the+ETC+Bill+%281%29.pdf/0a64ae18-b008-4bab-b86a-ed6adc244d25 (accessed 13 January 2023).
549 Communications Act 2009, available at: http://www.lac.org.na/laws/annoSTAT/Communications%20Act%208%20of%202009.pdf (accessed 13 January 2023).
550 Electronic Transactions Act, available at: http://www.lac.org.na/laws/2019/7068.pdf (accessed 13 January 2023).
551 Electronic Transactions and Cybercrime Act 2016, section 63, available at: https://mict.gov.na/documents/32978/0/Latest+Copy+of+the+ETC+Bill+%281%29.pdf/0a64ae18-b008-4bab-b86a-ed6adc244d25 (accessed13 January 2023).
552 Ibid, section 64.
553 Ibid, section 66.
554 Ibid, section 67.
555 Ibid, section 68.
556 Government Notice 292/2022

The National Security and Cyber Incidence Response Team (NSCIRT-Namibia) is a national computer emergency response team established to contribute to the security and stability of critical infrastructure and critical information infrastructure of the Republic of Namibia's institutions, bodies and agencies.[557]

F. National cybersecurity strategy
The National Cybersecurity Strategy and Awareness Raising Plan 2022–2027 outlines the strategy for addressing cybersecurity and mitigating gaps in curbing cybercrimes, with a vision to enhance security, enable innovation and develop resilient infrastructure.

G. Initiatives to combat cybercrime
- Namibia is one of the 195 INTERPOL [558] member countries.[559]
- The launch of a Cybersecurity Council to combat cyber fraud.[560] The council comprises information security experts and intends to give cybersecurity issues priority. There is also the Communications Regulatory Authority of Namibia, established by the Communications Act 2009.
- In the financial sector, the Bank of Namibia (BoN) requires that 'regulated entities are able to identify, measure and mitigate their exposure to the risk of losses attributed to cybercrime'. It ensures that both staff and customers are aware of the risks and their responsibilities pertaining to cybercrime prevention and cybersecurity by way of relevant staff training interventions and customer awareness.[561]
- Namibia has ratified the African Union Convention on Cyber Security and Personal Data Protection ('the Malabo Convention') 2014.

32. Nauru

A. National cyber threat landscape
Exact statistics and data on the cybercrime threat landscape were not available for Nauru on the National Cyber Security Index.

B. National cybercrime legislation and related laws
- Cybercrime Act 2015[562]

C. Scope/application of laws
The Cybercrime Act was enacted to provide for the prevention of, investigation, suppression and imposition of penalties for computer-related offences in Nauru and for other related purposes. Part 2 of the Act provides for computer-related offences such as illegal access,[563] illegal

557 National Security and Cyber Incidence Response Team, Communications Regulatory Authority of Namibia (CRAN), available at: https://www.cran.na/national-security-and-cyber-incidence-response-team/
558 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
559 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).
560 Xinhua (2022), 'Namibia Launches Cyber Security Council to Combat Cyber Fraud', available at: https://english.news.cn/20221121/137411e56b5b4724801983ba72ff703e/c.html#:~:text=WINDHOEK%2C%20Nov.,participants%20to%20combat%20cyber%20fraud (accessed 30 January 2023).
561 *The Namibian*, 'Cybercrime in Namibia', available at: www.namibian.com.na/index.php?page=archive-read&id=165301 (accessed 30 January 2023).
562 Cybercrime Act 2015, available at: http://ronlaw.gov.nr/nauru_lpms/files/acts/a59d9691f5a195412b877493a2a95e8b.pdf (accessed 16 January 2023).
563 Cybercrime Act 2015, section 6, available at: http://ronlaw.gov.nr/nauru_lpms/files/acts/a59d9691f5a195412b877493a2a95e8b.pdf (accessed 16 January 2023).

interception,[564] illegal data interference,[565] data espionage,[566] illegal system interference,[567] making, selling, distributing or possessing software or a device for committing a crime,[568] computer-related forgery,[569] computer-related fraud,[570] child pornography,[571] solicitation of children,[572] publishing of indecent or obscene information in electronic form,[573] identity-related crimes,[574] spam,[575] and disclosure of details of an investigation.[576]

D. Sanctions/penalties
The Cybercrimes Act provides the liability for computer-related offences in Part 2 of the Act as punishable, on conviction, to imprisonment for a period between five and ten years. It also provides the option of a fine between $30,000 and $100,000 Australian dollars, or both imprisonment and a fine in some cases.

E. National computer emergency response team (CERT)/computer security incident response team (CSIRT)
Nauru does not currently have an officially recognised CERT/CSIRT.

F. National cybersecurity strategy
The Nauru Government does not have a designated national cybersecurity strategy.

G. Initiatives to combat cybercrime

- The Nauru Ministry of Telecommunications is responsible for all government communications and information systems. Nauru introduced cybersecurity laws in 2015 for the first time.
- One of the government's initiatives in combatting cybercrime is by creation of awareness. The Nauru Police Force (NPF)[577] has been tasked with educating school students on the dangers of the internet. This is part of the 'community-wide cyber safety campaign which has been initiated by the Pacific Islands Chiefs of Police and developed by the Australian Federal Police'.[578] The campaign is called Cyber Safety Pasifika,[579] and was developed to highlight the risks of online bullying, predatory behaviour and crime.
- Nauru has a dedicated Cyber Security Awareness Team (CSAT)[580] as a part of the Information and Communications Technology Department[581] of the Nauru Ministry of Telecommunication.
- Nauru is also one of the 195 INTERPOL [582] member countries.[583]

564 Ibid, section 7.
565 Ibid, section 8.
566 Ibid, section 9.
567 Ibid, section 10.
568 Ibid, section 11.
569 Ibid, section 12.
570 Ibid, section 13.
571 Ibid, section 14.
572 Ibid, section 15.
573 Ibid, section 16.
574 Ibid, section 17.
575 Ibid, section 18.
576 Ibid, section 19.
577 The Government of the Republic of Nauru, NPF Organisational Structure, available at: http://naurugov.nr/government/departments/nauru-police-force/npf-organisational-structure.aspx (accessed 30 January 2023).
578 *FijiTimes* (2018), 'PACNEWS, Nauru Police Force Launches Cyber Safety Campaign', 10 May, available at: www.fijitimes.com/nauru-police-force-launches-cyber-safety-campaign/ (accessed 26 January 2023).
579 Cyber Safety Pasifika, Home, available at: www.cybersafetypasifika.org/ (accessed 26 January 2023).
580 Cyber Security Awareness Team, available at: www.nauru.gov.nr/government/departments/department-of-telecommunications/cyber-security-awareness-team.aspx (accessed 23 January 2023).
581 The Government of the Republic of Nauru, Department of ICT, available at: http://naurugov.nr/government/departments/department-of-telecommunications.aspx (accessed 30 January 2023).
582 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
583 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).

33. New Zealand

A. National cyber threat landscape

According to the National Cyber Security Index (NCSI),[584] as of January 2023 New Zealand ranked: 70th out of 161 countries on the NCSI with a score of 51.95; 48th out of 194 countries on the Global Cybersecurity Index; 13th on the ICT Development Index; and 19th on the Networked Readiness Index.

B. National cybercrime legislation and related laws

- Crime Act 1961[585]
- Film, Videos, and Publications Classifications Act 1993[586]
- Search and surveillance Act 2012[587]
- Mutual Assistance in Criminal Matters Act 1992[588]

C. Scope/application of laws

- The Crimes Act consolidates enactments relating to crimes and other offences in the country. It provides for crimes involving computers, such as accessing a computer system for dishonest purpose, interfering with a computer system, and unauthorised use or access of a computer system.[589]
- The Film, Videos, and Publications Classifications Act 1993 consolidates and amends the law relating to the censoring of films, videos, books and other publications.

D. Sanctions/penalties for cyber-related crimes

- The Crimes Act provides liability of a term of imprisonment from two to ten years for crimes involving computers.

E. National computer emergency response team (CERT)/computer security incident response team (CSIRT)

The National Computer Emergency Response Team of New Zealand (CERT NZ)[590] responds to cybersecurity threats in the country.

F. National cybersecurity strategy

The country has issued three cybersecurity strategies. The 2011 strategy outlined the government's response to cybercrime and established the National Cyber Security Centre and the National Cyber Policy Office. The 2015 strategy[591] had four goals: cyber resilience, cyber

584 NCSI: New Zealand, available at: https://ncsi.ega.nz/country/nz/ (accessed 17 January 2023).
585 New Zealand Legislation, Public Act, Crimes Act 1961 No. 43 (as at 06 November 2021), available at: www.legislation.govt.nz/act/public/1961/0043/latest/whole.html#DLM327382 (accessed 19 January 2023).
586 New Zealand Legislation, Public Act Contents, Films, Videos, and Publications Classification Act 1993 No. 94 (as at 12 April 2022), available at: www.legislation.govt.nz/act/public/1993/0094/latest/DLM312895.html?src=qs (accessed 19 January 2023).
587 New Zealand Legislation, Public Act Contents, Search and Surveillance Act 2012 No. 24 (as at 15 November 2022), available at: www.legislation.govt.nz/act/public/2012/0024/latest/DLM2136536.html?search=qs_act%40bill%40regulation%40deemedreg_Search+and+surveillance+Act+2012_resel_25_h&p=1&sr=1 (accessed 19 January 2023).
588 New Zealand Legislation, Public Act Contents, Mutual Assistance in Criminal Matters Act 1992 No. 86 (as at 28 October 2021), available at: www.legislation.govt.nz/act/public/1992/0086/latest/DLM273057.html (accessed 19 January 2023).
589 New Zealand Legislation, Public Act, Crimes Act 1961 No. 43 (as at 06 November 2021), sections 249–252, available at: www.legislation.govt.nz/act/public/1961/0043/latest/whole.html#DLM327382 (accessed 19 January 2023).
590 CERT NZ, available at: www.cert.govt.nz/ (accessed 26 January 2023).
591 Cybersecurity Strategy 2015, available at: https://dpmc.govt.nz/sites/default/files/2017-03/nz-cyber-security-strategy-december-2015.pdf (accessed 26 January 2023).

capability, addressing cybercrime and international co-operation. The 2019 strategy[592] outlines a wider scope and areas where the government needs to prioritise action to ensure a secure New Zealand.

G. Initiatives to combat cybercrime

- New Zealand is one of the 195 INTERPOL [593] member countries.[594]
- The National Plan to Address Cybercrime ('the Plan') was developed to support the cybercrime goal and contribute to the delivery of 'a secure, resilient and prosperous online New Zealand'.[595] It sets out the government's understanding of cybercrime; and to prevent, investigate, respond to and reduce harm to New Zealanders.
- Establishment of a New Zealand National Cyber Security Centre[596] (in the Government Communications Security Bureau), which monitors 'advanced threats against New Zealand's information infrastructures of national importance'.[597]
- Creation of the New Zealand Connect Smart initiative.[598] The initiative was launched in 2014 to promote awareness by creating ways for individuals, businesses and schools to protect themselves online; and to encourage a positive approach to cybersecurity.[599]
- Establishment of a range of government agencies to share responsibilities and combat cybercrime. These include the New Zealand Police Cybercrime Unit[600] and the New Zealand National Cyber Policy Office.[601]
- Ensuring continuous development and training of the police force in combatting cybercrime. For instance, the Police Prevention First: National Cybercrime Operating Strategy 2014–2017[602] sets out 'police goals to develop capacity and capability to meet the growing needs around cybercrime and cyber-enabled crime'.[603]
- Establishment of a New Zealand Cyber Credentials Scheme to help small businesses improve their cybersecurity.[604]

34. Nigeria

A. National cyber threat landscape

According to the National Cyber Security Index (NCSI),[605] as of January 2023 Nigeria ranked: 52nd on the NCSI with a score of 54.55; 47th on the Global Cybersecurity Index; 143rd on the ICT Development Index; and 103rd on the Networked Readiness Index.

592 New Zealand's Cyber Security Strategy 2019, available at: https://dpmc.govt.nz/publications/new-zealands-cyber-security-strategy-2019 (accessed 26 January 2023).
593 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
594 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).
595 National Plan to Address Cybercrime, available at: www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/nz-cyber-security-cybercrime-plan-december-2015.pdf (accessed 26 January 2023).
596 National Cyber Security Centre, Home, available at: www.ncsc.govt.nz/ (accessed 26 January 2023).
597 Ibid.
598 Connect Smart, available at: https://dpmc.govt.nz/our-programmes/special-programmes/connect-smart (accessed 26 January 2023).
599 Ibid.
600 New Zealand Police, Cybercrime, available at: www.police.govt.nz/advice-services/cybercrime-and-internet/cybercrime (accessed 26 January 2023).
601 National Cyber Policy Office, available at: https://dpmc.govt.nz/our-business-units/national-security-group/national-security-policy/national-cyber-policy-office (accessed 26 January 2023).
602 National Plan to Address Cybercrime, available at: www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/nz-cyber-security-cybercrime-plan-december-2015.pdf (accessed 26 January 2023).
603 Ibid.
604 *The Beehive*, 'Cyber Security Credentials Scheme Proposed for SMEs', available at: www.beehive.govt.nz/release/cyber-security-credentials-scheme-proposed-smes (accessed 26 January 2023).
605 NCSI: Nigeria, available at: https://ncsi.ega.ee/country/ng/ (accessed 14 January 2023).

B. National cybercrime legislation and related laws
- Cybercrime (Prohibiting, Prevention Etc.) Act 2015[606]
- Economic and Financial Crimes Commission (EFCC) (Establishment) Act 2004[607]
- Evidence Act 2011[608]
- Money Laundering (Prohibiting) Act 2011[609]
- Advance Fee Fraud and other Related Offences Act 2006

C. Scope/application of laws –
- The Cybercrime (Prohibition, Prevention, Etc.) Act, 2015 provides a framework for the prohibition, prevention, detection, prosecution and punishment of cybercrimes; and promotes cybersecurity and the protection of computer systems and networks, electronic communications, data, and computer programs. Part III of the Act prescribes offences and their penalties. These include unlawful access to a computer; unauthorised disclosure of an access code; data forgery; computer fraud; system interference; misuse of devices; denial of service; identity theft and impersonation; child pornography, grooming; cyberstalking; unlawful interception; cybersquatting; and cyber terrorism.[610]
- The Money laundering Act makes comprehensive provisions to prohibit the financing of terrorism, the laundering of the proceeds of a crime, or an illegal act; and provides appropriate penalties to such crimes.
- The EFCC (Establishment) Act mandates the EFCC to combat financial and economic crimes.

D. National computer emergency response team (CERT)/computer security incident response team (CSIRT)
The Nigeria CERT (ng-CERT)[611] seeks 'to manage the risks of cyber threats in Nigeria's cyber-space and effectively co-ordinate incident response and mitigation strategies to proactively prevent cyberattacks against Nigeria'.

E. National cybersecurity strategy
The current National Cybersecurity Policy and Strategy[612] was approved in 2021. The strategy 'articulates priorities, principles and approaches to understanding and managing cybersecurity risks at national level in Nigeria. It builds upon the previous Strategy and further provides cohesive measures and strategic initiatives towards assuring security of the cyberspace, safeguarding critical information infrastructures, as well as building and nurturing a trusted cybercommunity in Nigeria'.[613]

F. Initiatives to combat cybercrime
- Nigeria ratified the Convention on Cybercrime (ETS No. 185)[614] on 6 July 2022; it came into force in the country on 1 November 2022.[615]

---

606 Cybercrime Prohibition Prevention Act 2015, available at: www.cert.gov.ng/ngcert/resources/CyberCrime__Prohibition_Prevention_etc__Act__2015.pdf (accessed 13 January 2023).
607 Establishment Act, available at: www.efcc.gov.ng/about-efcc/the-establishment-act (accessed 14 January 2023).
608 Evidence Act, available at: http://www.placng.org/lawsofnigeria/laws/E14.pdf (accessed 13 January 2023).
609 Money Laundering Act 2011, available at: https://lawpadi.com/wp-content/uploads/2015/08/Money-Laundering-Act-2011.pdf (accessed 13 January 2023).
610 Cybercrime Prohibition Prevention Act 2015, sections 5–36, available at: www.cert.gov.ng/ngcert/resources/CyberCrime__Prohibition_Prevention_etc__Act__2015.pdf (accessed 13 January 2023).
611 ng-CERT, Home, available at: www.cert.gov.ng/ (accessed 15 January 2023).
612 National Security Policy and Strategy, available at: http://ctc.gov.ng/wp-content/uploads/2021/02/NATIONAL-CYBERSECURITY-POLICY-AND-STRATEGY-2021_E-COPY_24223825.pdf (accessed 26 February 2023).
613 Ibid.
614 Council of Europe, 'The Budapest Convention (ETS No. 185) and is Protocols', available at: www.coe.int/en/web/cybercrime/the-budapest-convention (accessed 26 January 2023).
615 Council of Europe, 'Complete list of Council of Europe's treaties', Treaty Office, available at: www.coe.int/en/web/conventions/full-list (accessed 25 January 2023).

- Nigeria is one of the 195 INTERPOL [616] member countries.[617]
- Approval of the Computer Crimes Prosecution Unit in the Nigeria Ministry of Justice,[618] as a specialised unit to combat cybercrime and related crimes and to prosecute the offenders.
- Establishment of units to combat cybercrime, such as the Nigerian Cybercrime Working Group, the Economic and Financial Crime Commission (EFCC)[619] and the Cybercrime Advisory Council.
- Establishment of the Nigerian Computer Emergency Response Team (ng-CERT)[620] to manage cyber threats in the country.

35. Pakistan

A. National cyber threat landscape

According to the National Cyber Security Index (NCSI),[621] as of January 2023 Pakistan ranked: 78th out of 161 countries on the NCSI with a score of 42.86; 79th out of 194 countries on the Global Cybersecurity Index; 148th on the ICT Development Index; and 97th on the Networked Readiness Index.

B. National cybercrime legislation and related laws

- Prevention of Electronic Crimes Act 2016 (PECA)[622]
- Prevention of Electronic Crime Ordinance (PECO)
- Electronic Transactions Ordinance 2002 (ETO)[623]
- Telecommunication (Reorganisation) Act 1996[624]
- Federal Investigation Agency Act 1974[625]
- Payments and Electronic Fund Transfers Act[626]

C. Scope/application of laws

- The Prevention of Electronic Crimes Act (PECA) makes provisions to prevent unauthorised acts to information systems, the prevention of electronic crimes and other related offences. It provides for cybercrimes such as unauthorised data access (hacking), denial of service (DoS), assault (DoS attack), unauthorised interception,[627] electronic forgery[628] and electronic fraud,[629] and cyberterrorism.
- The Federal Investigation Agency Act established the Federal Investigation Agency,[630] which investigates crimes at the national level in the country.

---

616 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
617 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).
618 Federal Ministry of Information and Culture, Federal Ministry of Justice Archives, available at: https://fmic.gov.ng/tag/federal-ministry-of-justice/ (accessed 27 January 2023).
619 Economic and Financial Crimes Commission, available at: www.efcc.gov.ng/ (accessed 27 January 2023).
620 ng-cert, Home, available at: www.cert.gov.ng/ (accessed 15 January 2023).
621 NCSI: Pakistan, available at: https://ncsi.ega.ee/country/pk/ (accessed 17 January 2023).
622 Prevention of Electronic Crimes Act, available at: https://na.gov.pk/uploads/documents/1470910659_707.pdf (accessed 7 January 2023).
623 Electronic Transaction Ordinance, available at: http://pklegal.shujaat.me/pdf/ETO-2002.pdf (accessed 7 January 2023).
624 Telecommunication (Re-Organisation) Act, available at: http://pklegal.shujaat.me/pdf/PTRA-1996.pdf (accessed 7 January 2023).
625 Federal Investigation Agency Act, available at: http://pklegal.shujaat.me/pdf/FIA-ACT-1974.pdf (accessed 7 January 2023).
626 Payments and Electronic Transfer Act, available at: http://pklegal.shujaat.me/pdf/EFT-2007-simple.pdf (accessed 7 January 2023).
627 Prevention of Electronic Crimes Act, section 17, available at: https://na.gov.pk/uploads/documents/1470910659_707.pdf (accessed 7 January 2023).
628 Ibid, section 11.
629 Ibid, section 12.
630 Federal Investigation Agency, available at: www.fia.gov.pk/ (accessed 15 January 2023).

D. Sanctions/penalties for cyber-related crimes
PECA imposes punishments of up to 3 months in prison, or maximum of 14 years' imprisonment and a fine of 50 million Pakistani rupees, or both.

E. National computer emergency response team (CERT)/computer security incident response team (CSIRT)
Pakistan has a National Response Centre for Cyber Crime (NR3C).[631]

F. National cybersecurity strategy
The National Cybersecurity Policy 2021[632] was developed to address the cybersecurity challenges and risk factors faced by Pakistan, including through establishing a governance framework, addressing the importance of information systems and critical infrastructure, and by building capacity.

G. Initiatives to combat cybercrime
- Pakistan is one of the 195 INTERPOL [633] member countries.[634]
- Establishment of Cyber Crime Reporting Centres in 15 cities in Pakistan. Citizens can also exercise the right to report cybercrimes by submitting complaints and reports of cybercrime incidents online.[635]
- The creation of the Pakistan Cybercrime Investigation Portal[636] allows for ease and fast reporting and investigation of cybercrimes, and a resulting quick apprehension of cyber criminals.
- Inception of the Cybercrime Wing (CCW) of the Federal Investigation Agency (FIA)[637] in 2007 allows the FIA more coverage in tackling cybercrime in the country.

36. Papua New Guinea

A. National cyber threat landscape
According to the National Cyber Security Index (NCSI),[638] as of January 2023 Papua New Guinea ranked: 116th out of 161 countries on the NCSI with a score of 22.08; and 118th out of 194 countries on the Global Cybersecurity Index.

B. National cybercrime legislation and related laws
- Cybercrime Code Act 2016[639]
- National Information and Communication Technologies Act 2009[640]

C. Scope/application of laws
- The Cybercrime Code Act defines and establishes offences constituting cybercrime. Part III of the Act provides for offences and penalties. Division 1 thereof provides for offences relating to the integrity of data and electronic systems or devices, such as unauthorised access or hacking, illegal interception, data interference, system interference and data espionage. Division 2 provides for computer-related offences such as electronic fraud, forgery, gambling, identity theft and illegal devices. Division 3 provides for content-related

631 National Response Centre for Cyber Crime, available at: https://nr3c.gov.pk/ (accessed 23 January 2023).
632 Digital Pakistan Cybersecurity Policy, National Cyber Security Policy 2021, available at: https://moitt.gov.pk/SiteImage/Misc/files/National Cyber Security Policy 2021 Final.pdf
633 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
634 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).
635 Federal Investigation Agency, available at: www.fia.gov.pk/> accessed 15 January 2023).
636 National Response Centre for Cyber Crime, available at: https://nr3c.gov.pk/ (accessed 23 January 2023).
637 Federal Investigation Agency, available at: www.fia.gov.pk/ (accessed 23 January 2023).
638 NCSI: Papua New Guinea, available at: https://ncsi.ega.ee/country/pg/ (accessed 17 January 2023).
639 Cyber Code Act, available at: www.parliament.gov.pg/uploads/acts/16A_35.pdf (accessed 16 January 2023).
640 National Information and Communication Technologies Act 2009, available at: www.nicta.gov.pg/legislative/acts/ (accessed 15 January 2023).

offences such as pornography, child pornography, cyber bullying, cyber harassment, cyber extortion, unlawful disclosure and spam. Division 4 provides for other offences such as cyberattack.

- The National Information and Communication Technologies Act establishes the National Information and Communications Technology Authority and regulates the ICT industry.

D. National computer emergency response team (CERT)/computer security incident response team (CSIRT)
The Papua New Guinea Computer Emergency Response (PNGCERT)[641] 'works to promote awareness, provide advisory assistance and co-ordinate responses to cyber-security incidents in the country'.

E. National cybersecurity strategy
Papua New Guinea has a National Cyber Security Policy that delineates and describes the policy for Papua New Guinea (PNG) and sets out the government's approach towards addressing cybersecurity. [642]

F. Initiatives to combat cybercrime
- Papua New Guinea is one of the 195 INTERPOL [643] member countries.[644]
- The National ICT Policy 2008[645] provides the policy foundation for non-permission of cybercrime in Papua New Guinea.
- The formation of the Papua New Guinea Core Working Group (CWG) in 2010, which has officers from the National Information and Communication Technology Authority (NICTA),[646] and the Department of Justice[647] and Attorney General, for the creation of the country's Cybercrime Policy 2014.[648] The NICTA is the exercising authority for the relevant laws.
- The Cybercrime Policy 2014[649] specifically provides for cybercrime and was formally endorsed by Cabinet through NEC Decision No. 219/2014. It highlights the need to develop a legal framework that criminalises cybercrime in the country, while also calling for the strengthening of collaboration and partnerships with specialised regional and international agencies and governments on cybercrime.[650]
- International co-operation and attendance of cybercrime workshops. For instance, the Pacific Islands cybercrime workshops[651] held in the Republic of Vanuatu, Samoa and the Kingdom of Tonga.

641 Papua New Guinea Computer Emergency Response Team, available at: www.nicta.gov.pg/regulatory/internet/pngcert/ (accessed 16 January 2023).
642 Papua New Guinea National Cyber Security Policy National Cybersecurity Policy 2021 (Final), available at: https://www.ict.gov.pg/Policies/Cyber Security Policy/NATIONAL CYBERSECURITY POLICY 2021 (Final) - 031121- PRINT.pdf
643 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
644 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).
645 National ICT Policy, available at: www.kch.com.pg/wp-content/uploads/2019/03/National-ICT-Policy-Aprill-2008.pdf (accessed 24 January 2023).
646 National ICT Authority of Papua New Guinea, available at: www.nicta.gov.pg/ (accessed 30 January 2023).
647 DJAG, Home, available at: www.justice.gov.pg/ (accessed 30 January 2023).
648 Cybercrime Policy 2014, available at: www.nicta.gov.pg/download/cybercrime-policy-2014/?tmstv=1674057359 (accessed 15 January 2023).
649 Cybercrime Policy 2014, available at: www.nicta.gov.pg/download/cybercrime-policy-2014/?tmstv=1674057359> accessed 15 January 2023).
650 Ibid.
651 Cybercrime Working Group, Pacific Islands Law Officers Network (PILON), available at: https://pilonsec.org/our-work/working-groups/cybercrime/ (accessed 30 January 2023).

37. Rwanda

A. National cyber threat landscape

According to the National Cyber Security Index (NCSI),[652] as of January 2023 Rwanda ranked: 92nd on the NCSI with a score of 33.77; 57th on the Global Cybersecurity Index; 153rd on the ICT Development Index; and 101st on the Networked Readiness Index.

B. National cybercrime legislation and related laws

- Law No. 60/2018 OF 22/8/2018 on Prevention and Punishment of Cyber Crimes[653]
- Law No. 058/2021 of 13/10/2021 Relating to the Protection of Personal Data and Privacy (the 'Data Protection Law')
- Law No. 24/2016 of 18/06/2016 Governing Information and Communication Technologies in Rwanda (the 'ICT Law')

C. Scope/application of laws

- Chapter IV of the Law on Prevention and Punishment of Cyber Crimes provides for offences and penalties as follows. Article 16: unauthorised access to a computer or a computer system data; Article 17: access to data with intent to commit an offence; Article 18: unauthorised modification of computer or computer system data; Article 19: interception of a computer; Article 27: cybersquatting; Article 32: computer- or computer system-related forgery; Article 34: publication of pornographic images through a computer or a computer system; Article 35: cyber-stalking; Article 36: phishing Article 37: spamming; and Article 38: publishing indecent information in electronic form.

D. National computer emergency response team (CERT)/computer security incident response team (CSIRT)

The Rwanda Development Board under the ICT Department established the Rwanda Computer Security Incident Response Team (Rw-CSIRT) in August 2014. Rw-CSIRT is now operating under the National Cyber Security Authority (NCSA).[654]

E. National cybersecurity strategy

Rwanda has a National Cyber Security Strategic Plan 2015,[655] which provides implementation guidance for the defined National Cyber Security Policy (NCSP) 2015. It is the NCSP that defines the establishment of a strong and effective cybersecurity governance in the country, which provides strong leadership in national cybersecurity and information security programmes.

F. Initiatives to combat cybercrime

- Rwanda is one of the 195 INTERPOL [656] member countries.[657]
- From 28 February to 3 March, Rwanda hosted the 2023 FIRST and AfricaCERT Symposium for cybersecurity practitioners from Africa and the Arab regions. The symposium was co-organised by the Forum for Incident Response and Security Teams (FIRST), the African Forum of Computer Incident Response Teams (AfricaCERT), and the Rwandan National Cyber Security Authority (NCSA).[658]

652 NCSI: Rwanda, available at: https://ncsi.ega.ee/country/rw/ (accessed 14 January 2023).
653 Law No. 60/2018 of 22/8/2018 on Prevention and Punishment of Cyber Crimes, available at: www.risa.rw/fileadmin/user_upload/Others%20documents/Cyber_Crimes_Law.pdf (accessed 13 January 2023).
654 NCSA, RW-CSIRT, available at: https://cyber.gov.rw/rw-csirt/ (accessed 15 January 2023).
655 National Cyber Security Strategic Plan 2015, available at: https://www.risa.rw/fileadmin/user_upload/Others documents/National_Cyber_Security_Strategic_Plan_Rwanda.pdf
656 The Internation al Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
657 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).
658 National Cyber Security Authority, 'Rwanda hosts the 2023 FIRST and AfricaCERT Symposium: Africa and Arab regions', available at: https://cyber.gov.rw/updates/article/rwanda-hosts-the-2023-first-and-africacert-symposium-for-africa-and-the-arab-regions/

- The establishment of the NCSA, which was operationalised in 2020 by virtue of Law No. 26/2017 of 31 May 2017. The NCSA co-ordinates national cybersecurity functions across the private and public sectors, to ensure the security and resilience of Rwanda's ICT ecosystem, as well as promoting national education programmes and fostering awareness of cybersecurity best practices.[659]
- Rwanda has ratified the African Union Convention on Cyber Security and Personal Data Protection ('the Malabo Convention') 2014.

38. Saint Lucia

A. National cyber threat landscape
According to the National Cyber Security Index (NCSI),[660] as of January 2023 Saint Lucia ranked: 136th out of 161 countries on the NCSI with a score of 12.99; 158th out of 194 countries on the Global Cybersecurity Index; and 104th on the ICT Development Index.

B. National cybercrime legislation and related laws
- Criminal Code, Act 9 of 2004[661]
- Electronic Transactions Act, No. 16 of 2011[662]

C. Scope/application of laws
- The Criminal Code provides for criminal offences and procedure and for matters incidental thereto. Section 267 of the Act provides for computer fraud. It states that: 'A person who, with intent to defraud or deceive: (a) alters, damages, destroys or otherwise manipulates data or programs held in or used in connection with a computer or computer network by adding to, erasing or otherwise altering the data or programme; or (b) does any act which causes an unauthorised modification of the contents of a computer or computer network; commits an offence.'

D. Sanctions/penalties for cyber-related crimes
- By the provisions of the Criminal Code, computer fraud is punishable on conviction on indictment to imprisonment for 15 years.

E. National computer emergency response team (CERT)/computer security incident response team (CSIRT)
There is no record of a national CERT in Saint Lucia.

F. National cybersecurity strategy
Saint Lucia does not have any officially approved national or sector-specific cybersecurity strategy for implementing cybersecurity standards.

G. Initiatives to combat cybercrime
- Saint Lucia is a member of the Caribbean Community (CARICOM).
- Saint Lucia is one of the 195 INTERPOL [663] member countries.[664]

659 National Cyber Security Authority, available at: https://cyber.gov.rw/about/
660 NCSI: Saint Lucia, available at: https://ncsi.ega.ee/country/lc/ (accessed 14 January 2023).
661 Criminal Code, available at: www.govt.lc/media.govt.lc/www/resources/legislation/Criminal%20Code.pdf (accessed 15 January 2023).
662 Electronic Transactions Act, available at: https://issuu.com/amlregulator/docs/electronic_transactions_act_st_luci (accessed 13 January 2023).
663 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
664 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).

c. Formation of a national E-Government Taskforce,[665] which reviewed legislation and policies and developed an acceptable use policy for e-government services. It is said to have laid a good foundation for 'managing the country's cybersecurity/crime environment, as well as the plan for establishing the CERT'.[666]

39. Samoa

A. National cyber threat landscape
According to the National Cyber Security Index (NCSI),[667] as of January 2023 Samoa ranked: 143rd out of 161 countries on the NCSI with a score of 10.39; 111th out of 194 countries on the Global Cybersecurity Index; and 127th on the ICT Development Index.

B. National cybercrime legislation and related laws
- Crimes Act 2013[668]
- Electronic Transactions Act 2008[669]

C. Scope/application of laws
- The Crimes Act regulate crimes in Samoa. Part XVIII of the Act provides for crimes involving electronic systems. It provides for offences such as accessing an electronic system without authorisation; accessing an electronic system for dishonest purpose; illegal remaining in an electronic system; illegal interception; damaging or interfering with electronic data; illegal acquisition of electronic data; illegal system interference; illegal devices; making, selling, distributing or possessing software for committing a crime; identity fraud; forgery of electronic data; spamming; solicitation of children; and harassment utilising means of electronic communication.[670]
- The Electronic Transactions Act facilitates the use of electronic transactions and for matters connected thereto.

D. Sanctions/penalties for cyber-related crimes
- The Crimes Act prescribes penalties for crimes involving electronic systems. They range from imprisonment between five and ten years. It further includes the payment of a fine of not more than 100 penalty units for spamming.

E. National computer emergency response team (CERT)/computer security incident response team (CSIRT)
The Samoa Computer Emergency Response Team (SamCERT) is Samoa's national cybersecurity agency and provides response, awareness, support and assistance on cybersecurity threats and incidents. SamCERT also represents Samoa as the main technical body for cybersecurity on regional and international engagements and collaboration to develop policies and improve standards on cybersecurity.

F. National cybersecurity strategy
The Samoa National Cyber Security Strategy 2016–2021 was launched in 2017.[671]

---

665 Government of Saint Lucia (2009), 'E-Government Drive Continues to Enhance Public Service', available at: https://archive.stlucia.gov.lc/pr2009/june/e_government_drive_continues_to_enhance_public_service.htm (accessed 30 January 2023).
666 PublicTechnology.net (2022), 'No one is an island: how Caribbean states are working together to tackle cybercrime', 17 October, available at: https://publictechnology.net/articles/features/no-one-island-how-caribbean-states-are-working-together-tackle-cybercrime (accessed 24 January 2023).
667 NCSI: Samoa, available at: https://ncsi.ega.ee/country/ws/ (accessed 14 January 2023).
668 Crimes Act 2013, available at: https://sherloc.unodc.org/cld/uploads/res/document/wsm/2013/crimes_act_2013_html/Samoa_Crimes_Act_2013.pdf (accessed 14 January 2023).
669 Electronic Transactions Act, available at: www.wipo.int/edocs/lexdocs/laws/en/ws/ws010en.pdf (accessed 16 January 2023).
670 Crimes Act 2013, sections 206–219, available at: https://sherloc.unodc.org/cld/uploads/res/document/wsm/2013/crimes_act_2013_html/Samoa_Crimes_Act_2013.pdf (accessed 14 January 2023).
671 MCIT (2017), Samoa National Cybersecurity Strategy 2016–2021.pdf, available at: https://www.samoagovt.ws/wp-content/uploads/2017/02/MCIT-Samoa-National-Cybersecurity-Strategy-2016-2021.pdf

G. Initiatives to combat cybercrime
- Samoa is one of the 195 INTERPOL [672] member countries.[673]
- International co-operation, attendance and hosting of cybercrime workshops; for instance, the Pacific Islands Law Officers' Network (PILON) cybercrime workshop[674] was hosted by Samoa.

40. Seychelles

A. National cyber threat landscape
According to the National Cyber Security Index (NCSI),[675] as of January 2023 Seychelles ranked: 148th on the NCSI with a score of 10.39; 149th on the Global Cybersecurity Index; and 90th on the ICT Development Index.

B. National cybercrime legislation and related laws
- The Computer Misuse (Amendment) Act 2012[676]
- Computer Misuse Act (CMA) 1998[677]
- Electronic Transactions Act (ETA) 2011[678]

C. Scope/application of laws
- The CMA provides for computer-related offences such as unauthorised access to a computer, unauthorised access with criminal intent and unauthorised modification of computer material.[679]
- The ETA provides for the legal recognition of transactions carried out by means of electronic data interchange and other means of electronic communication.

D. Sanctions/penalties for cyber-related crimes
- A person found guilty of a cyber offence under the CMA is liable on conviction to a fine between 10,000 and 30,000 Seychelles rupee (SRs) and to imprisonment between two and five years[680]
- Part IX of the ETA provides for offences. Section 42 thereof prescribes the punishment of imprisonment for three years and a fine of SRs20,000 for concealing, destroying or altering, or causing another to conceal, destroy or alter, any computer source code.

E. National computer emergency response team (CERT)/computer security incident response team (CSIRT)
There is no record of a national CERT in Seychelles.

F. National cybersecurity strategy
Seychelles does not have any officially approved national or sector-specific cybersecurity strategy for implementing cybersecurity standards.

---

672 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
673 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).
674 Cybercrime Working Group, Pacific Islands Law Officers Network (PILON), available at: https://pilonsec.org/our-work/working-groups/cybercrime/ (accessed 30 January 2023).
675 NCSI: Seychelles, available at: https://ncsi.ega.ee/country/sc/ (accessed 14 January 2023).
676 Seychelles Computer Misuse (Amendment) Act 2012, p.1, ICT Policy Africa, available at: https://ictpolicyafrica.org/es/document/oopq6nfsuth (accessed 15 January 2023).
677 Seychelles Computer Misuse Act, 1998, p.3, ICT Policy Africa, available at: https://ictpolicyafrica.org/es/document/annbbkm3ca?page=3 (accessed 15 January 2023).
678 Electronic Transactions Act 2011, available at: https://lawstrust.com/sites/default/files/docs/juris_laws/Electronic_Transactions_Act_2001.pdf (accessed 13 January 2023).
679 Articles 3, 4 and 5 Seychelles Computer Misuse Act, 1998, p.3, ICT Policy Africa, available at: https://ictpolicyafrica.org/es/document/annbbkm3ca?page=3 (accessed 15 January 2023).
680 The Seychelles Computer Misuse Act, 1998, p.3, ICT Policy Africa, available at: https://ictpolicyafrica.org/es/document/annbbkm3ca?page=3 (accessed 15 January 2023).

G. Initiatives to combat cybercrime
- Seychelles is one of the 195 INTERPOL [681] member countries.[682]
- Creation of the National ICT Policy,[683] which contains policy objectives such as improving Seychelles ICT infrastructure, and legal and regulatory framework objectives, which cover computer and computer-related crime and security.[684]

41. Sierra Leone

A. National cyber threat landscape
According to the National Cyber Security Index (NCSI),[685] as of January 2023 Sierra Leone ranked: 154th on the NCSI with a score of 7.79; and 121st on the Global Cybersecurity Index.

B. National cybercrime legislation and related laws
- The Cybercrime Act 2020[686]
- Cybersecurity and Cybercrimes Act 2021
- Telecommunication Act 2006

C. Scope/application of laws
- The Cybercrime Act provides for the prevention of the abusive use of computer systems and for the timely and effective collection of electronic evidence for the purpose of investigation and prosecution of cybercrime. Part V of the Act makes provision for cyber offences such as unauthorised access to a protected system, unauthorised data interception, unauthorised data and system interference, computer-related forgery, computer fraud, identity theft and impersonation, cyber stalking and cyber bullying, cybersquatting, online child sexual abuse, and cyber terrorism.[687]

D. National computer emergency response team (CERT)/computer security incident response team (CSIRT)
There is no record of a national CERT in Sierra Leone.

E. National cybersecurity strategy
Sierra Leone's National Cyber Security and Data Protection Strategy 2017–2022[688] (draft) is intended to shape the government's policy on cybersecurity and stipulate a vision to promote cybersecurity at all levels, including for the public and private sectors, civil society, academia and the wider population.

F. Initiatives to combat cybercrime
- Sierra Leone is one of the 195 INTERPOL [689] member countries.[690]
- Establishment of a Cybercrime Unit in the Criminal Investigation Department, to specifically investigate and prosecute computer- and internet-related crimes.

---

681 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
682 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).
683 National ICT Policy, available at: http://www.ict.gov.sc/resources/policy.pdf (accessed 23 January 2023).
684 Council of Europe, 'Octopus Cybercrime Community', Asset Publisher, available at: www.coe.int/en/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/seychelles/pop_up (accessed 30 January 2023).
685 NCSI: Sierra Leone, available at: https://ncsi.ega.ee/country/sl/ (accessed 14 January 2023).
686 Cyber Crime Act 2020, available at: http://www.sierra-leone.org/Laws/2020-Cybercrime%20Act.pdf (accessed 13 January 2023).
687 Cyber Crime Act 2020, sections 25–41, available at: http://www.sierra-leone.org/Laws/2020-Cybercrime%20Act.pdf (accessed 13 January 2023).
688 Sierra Leone's National Cyber Security and Data Protection Strategy 2017–2022, available at: www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/00090_03_Sierra Leone national-cyber-security-strategy-2017-final-draft.pdf
689 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
690 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).

42. Singapore

A. National cyber threat landscape
According to the National Cyber Security Index (NCSI),[691] as of January 2023 Singapore ranked: 28th out of 161 countries on the NCSI with a score of 71.43; 4th out of 194 countries on the Global Cybersecurity Index; 18th on the ICT Development Index; and 2nd on the Networked Readiness Index.

B. National cybercrime legislation and related laws
- The Computer Misuse Act 1993[692]
- Cybersecurity Act No.9/ 2018[693]
- Electronic Transactions Act 2010[694]

C. Scope/application of laws
- The Computer Misuse Act (CMA) is the principal legislation on cybercrimes in the country. It makes provision for securing computer material against unauthorised access or modification and for matters related thereto. Part 2 of the Act provides for offences such as unauthorised access to computer material, access with intent to commit or facilitate commission of an offence, unauthorised modification of computer material, unauthorised use or interception of a computer service, unauthorised obstruction of use of a computer, and unauthorised disclosure of an access code.
- The Cybersecurity Act authorises the taking of measures to prevent, manage and respond to cybersecurity threats and incidents, to regulate owners of critical information infrastructure, to regulate cybersecurity service providers, and for matters related thereto.
- The Electronic Transactions Act provides for the security and use of electronic transactions.

D. Sanctions/penalties for cyber-related crimes
- The Computer Misuse Act prescribes punishment ranging from a fine of $5,000 to $50,000 Singapore dollars, and terms of imprisonment from two to ten years for computer-related offences. It further prescribes enhanced punishment for offences involving protected computers,[695] with a fine not exceeding $100,000 Singapore dollars or to imprisonment for a term not exceeding 20 years, or to both a fine and imprisonment.

E. National computer emergency response team (CERT)/computer security incident response team (CSIRT)
The Singapore Computer Emergency Response Team (SingCERT) responds to cybersecurity incidents.

F. National cybersecurity strategy
The Singapore Cybersecurity Strategy 2021[696] outlines updated cybersecurity goals for the country and provides different approaches to adapt to the evolving digital world. It is a revision of the country's strategy that was first launched in 2016. The three strategic pillars of the revised strategy are: building resilient infrastructure, enabling a safe cyberspace and enhancing international cyber co-operation.

691 NCSI: Singapore, available at: https://ncsi.ega.ee/country/sg/ (accessed 14 January 2023).
692 Singapore Statutes Online, Computer Misuse Act 1993 , available at: https://sso.agc.gov.sg:5443/Act/CMA1993?ProvIds=P12- (accessed 19 January 2023).
693 Singapore Statutes Online, Cybersecurity Act 2018 , available at: https://sso.agc.gov.sg:5443/Acts-Supp/9-2018/ (accessed 19 January 2023).
694 Singapore Statues Online, Electronic Transactions Act 2010, available at: https://sso.agc.gov.sg:5443/Act/ETA2010 (accessed 19 January 2023).
695 Singapore Statutes Online, Section 11, Computer Misuse Act 1993, available at: https://sso.agc.gov.sg:5443/Act/CMA1993?ProvIds=P12- (accessed 19 January 2023).
696 Cyber Security Agency (2021), Singapore Cybersecurity Strategy 2021, available at: www.csa.gov.sg/News/Publications/singapore-cybersecurity-strategy-2021 (accessed 19 January 2023).

G. Initiatives to combat cybercrime

- Singapore is one of the 195 INTERPOL [697] member countries.[698]
- Publication of the country's National Cybercrime Action Plan (NCAP), which sets out the 'Government's key principles and priorities in combatting cybercrime. It also details the Government's ongoing efforts, as well as future plans, to effectively deal with cybercrime'.[699] The key principles that underpin the action plan are: prevention of cybercrimes, providing agile responses to cybercrime threats, a robust criminal justice system and shared responsibility for combatting cybercrimes.[700]
- International co-operation by working with foreign countries.
- Establishment of the Association of Southeast Asian Nations (ASEAN) Senior Officials Meeting on Transnational Crime (SOMTC) Working Group on Cybercrime in 2013. This serves as a platform for ASEAN member states to collaborate and co-ordinate efforts on 'capacity building, training and the sharing of information to combat cybercrime'.[701]
- Offering cybersecurity to the masses through, for instance, the provision of national internet infrastructure and mobile tools for Singaporeans to secure their smartphones from cybersecurity threats.[702]
- Launch of a Cyber Safe Programme[703] by the Cyber Security Agency of Singapore, to help enterprises improve their cybersecurity awareness.
- Working with and leading efforts within INTERPOL ,[704] such as the INTERPOL Global Complex for Innovation (IGCI),[705] to ensure the presence of operational frameworks to combat cybercrime.
- Establishment of the Cyber Security Agency of Singapore.[706]
- Building capacities at the regional and international levels, for example the ASEAN Cyber Capacity Development Project,[707] funded by Japan and implemented by INTERPOL, and the Singapore–United States Third Country Training Programme.[708]
- Driving thought leadership platforms for multi-stakeholder, regional and international dialogues on cybercrime, for example, the annual Asia Pacific's leading conference on information security (RSA Conference Asia Pacific and Japan).[709]

---

697 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
698 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).
699 National Cybercrime Action Plan, available at: www.mha.gov.sg/docs/default-source/media-room-doc/ncap-document.pdf (accessed 27 January 2023).
700 Ibid.
701 Ibid.
702 *The Straits Times* (2021), 'New govt cyber-security tool being developed to protect Singaporeans' phones from hackers', Singapore, 5 October, available at: www.straitstimes.com/tech/tech-news/new-govt-cyber-security-tool-being-developed-to-protect-singaporeans-phones-from (accessed 26 January 2023).
703 OpenGov Asia (2021), 'Cyber Security Agency of Singapore launches programme to help companies strengthen cybersecurity', 4 March, available at: https://opengovasia.com/cyber-security-agency-of-singapore-launches-programme-to-help-companies-strengthen-their-cybersecurity/ (accessed 26 January 2023).
704 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
705 INTERPOL (2014), 'INTERPOL Global Complex for Innovation opens its doors', available at: www.interpol.int/News-and-Events/News/2014/INTERPOL-Global-Complex-for-Innovation-opens-its-doors (accessed 26 January 2023).
706 Cyber Security Agency of Singapore (CSA), available at: www.csa.gov.sg/ (accessed 19 January 2023).
707 ASEAN Capacity Project, available at: https://jaif.asean.org/project-brief/asean-cyber-capacity-development-project-phase-ii/ (accessed 23 January 2023).
708 Government of Singapore (2018), Singapore–United States Third Country Training Programme, available at: http://www.mfa.gov.sg/Newsroom/Announcements-and-Highlights/2018/08/TCTPsigning (accessed 26 January 2023).
709 Asia Pacific Conference, available at: www.rsaconference.com/apj (accessed 23 January 2023).

43. Solomon Islands

A. National cyber threat landscape

According to the National Cyber Security Index (NCSI),[710] as of January 2023 Solomon Islands ranked: 159th out of 161 countries on the NCSI with a score of 2.60; 166th out of 194 countries on the Global Cybersecurity Index; and 157th on the ICT Development Index.

B. National cybercrime legislation and related laws

- Telecommunications Act 2009[711]
- The Criminal Procedure Code[712]

C. Scope/application of laws

- The Telecommunications Act amends and consolidates the law relating to telecommunications. Part IV of the Act sets out offences such as unlicensed telecommunications,[713] tampering with telecommunications, altering a message,[714] fraudulently transmitting messages,[715] impeding messages,[716] fraudulent retention of messages,[717] a forged telegram[718] and other offences in connection with telecommunications.[719]
- The Criminal Procedure Code makes provision for the procedure to be followed in criminal cases.

D. Sanctions/penalties

- The Telecommunications Act provides penalties ranging from a fine of SI$20 to 500 Solomon Island dollars, or to imprisonment between one month and three years, or to both such fine and such imprisonment.

E. National computer emergency response team (CERT)/computer security incident response team (CSIRT)

Solomon Islands does not currently have an officially recognised CERT.

F. National cybersecurity strategy

The Solomon Islands government does not have a designated national cybersecurity strategy. However, the National Security Strategy[720] is the country's first security strategy, having been introduced in October 2020. It seeks to ensure 'capabilities to protect the country's security are credible and can be respected'. It has among its strategic goals, the development of information security and cybersecurity capabilities; and it emphasises the importance of 'building public–private partnership and capacity to strengthen measures against cyber threats'.[721]

G. Initiatives to combat cybercrime

- Solomon Island is one of the 195[722] member countries.[723]

---

710 NCSI: United Kingdom, available at: https://ncsi.ega.ee/country/uk/ (accessed 14 January 2023).
711 Telecommunications Act, available at: http://www.paclii.org/sb/legis/consol_act/ta214/ (accessed 30 January 2023).
712 Criminal Procedure Code, available at: http://www.paclii.org/sb/legis/consol_act/cpc190/ (accessed 30 January 2023).
713 Telecommunications Act, section 21, available at: http://www.paclii.org/sb/legis/consol_act/ta214/ (accessed 30 January 2023).
714 Ibid, section 25.
715 Ibid, section 26.
716 Ibid, section 27.
717 Ibid, section 29.
718 Ibid, section 32.
719 Ibid, section 33.
720 National Security Strategy, available at: https://pacificsecurity.net/wp-content/uploads/2021/03/210201-SOLOMONS-National-Security-Strategy-Final_.pdf (accessed 25 January 2023).
721 Ibid.
722 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
723 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).

- 'Cyber Smart Pacific'[724] is a governmental initiative that creates awareness by 'encouraging all Solomon Islanders to Cyber Up and increase their cyber resilience so they're less vulnerable to attacks'. The initiative helps raise cybersecurity awareness among the public.
- Formulation of the National ICT Policy,[725] which sets out an action plan related to cybercrime and mainly: 'to ensure appropriate legal protection for the community at large from potential ICT-related risks; ensure regulatory, law enforcement and judicial personnel have the skills and resources required to administer and enforce ICT laws effectively'. It mentions the significance of cybersecurity measures in enabling a protective ICT framework.
- Co-operation and collaboration on cybersecurity matters, such as the 'Cyber Safety Pasifika'[726] initiative, which is a partnership between the Australian Federal Police and the Pacific Islands Chiefs of Police to be proactive in preventing cybercrime in the Pacific region.
- Organising trainings and awareness workshops. Through this, an agency like the Royal Solomon Islands Police Force (RSIPF) has '35 trained officers across all the provinces who can deliver a cyber safety awareness presentation to their communities'.[727]

44. Sri Lanka

A. National cyber threat landscape

According to the National Cyber Security Index (NCSI),[728] as of January 2023 Sri Lanka ranked: 79th out of 161 countries on the NCSI with a score of 42.86; 83rd out of 194 countries on the Global Cybersecurity Index; 117th on the ICT Development Index; and 78th on the Networked Readiness Index.

B. National cybercrime legislation and related laws

- Cybersecurity Act of 2019[729]
- Electronic Transactions Act, No. 19 of 2006[730]
- Computer Crime Act No. 24 2007[731]
- Payment Devices Frauds Act 2006[732]

C. Scope/application of laws

- The Cybersecurity Act provides for: 'the implementation of the national cybersecurity strategy of Sri Lanka; to provide for the establishment of the digital infrastructure protection agency of Sri Lanka; to provide for the empowerment of the Sri Lanka computer emergency readiness team and other institutional framework; to protect critical information infrastructure within Sri Lanka; and to provide for matters connected therewith or incidental thereto'.

724 Cyber Smart Pacific, available at: https://solomons.gov.sb/cyber-smart-pacific/ (accessed 30 January 2023).
725 National ICT Policy, available at: http://www.mca.gov.sb/resources/national-policies/10-national-ict-policy/file.html (accessed 23 January 2023).
726 Cyber Safety Pasifika, Home, available at: http://www.cybersafetypasifika.org/ (accessed 30 January 2023).
727 Royal Solomon Islands Police Force (RSIPF), Reminds Public about Cyber Crimes, available at: www.rsipf.gov.sb/?q=node/1490 (accessed 30 January 2023).
728 NCSI: Solomon Islands, available at: https://ncsi.ega.ee/country/sb/ (accessed 14 January 2023).
729 Cybersecurity Act 2019, available at: www.cert.gov.lk/documents/Cyber%20Security%20Bill.pdf (accessed 16 January 2023).
730 Electronic Transactions Act, No. 19 of 2006, available at: www.gov.lk/elaws/wordpress/wp-content/uploads/2015/07/ElectronicTransactionActNo19of2006.pdf (accessed 23 January 2023).
731 Computer Crime Act, available at: https://sherloc.unodc.org/cld/uploads/res/document/lka/computer_crimes_act_html/Sri_Lanka_Computer_Crimes_Act_2007.pdf (accessed 16 January 2023).
732 Payment Devices Frauds Act (No. 30 of 2006), section 3, available at: http://www.commonlii.org/lk/legis/num_act/pdfa30o2006277/s3.html (accessed 19 January 2023).

- The Electronic Transactions Act: 'recognizes and facilitates the formation of contracts, the creation and exchange of data messages, electronic documents, electronic records and other communications in electronic form in Sri Lanka; and to provide for the appointment of a certification authority and accreditation of certification service providers; and to provide for matters connected therewith or incidental thereto'.
- The Computer Crime Act provides for the identification of computer crime and provides the procedure for the investigation and prevention of such crimes; and provides for matters connected therewith and incidental thereto. Part I of the Act provides for computer crimes such as securing unauthorised access to a computer, causing a computer to perform a function without lawful authority, illegal interception of data, use of illegal devices and unauthorised disclosure of information enabling access to a service.
- Section 3 of the Payment Devices Frauds Act provides for acts amounting to payment devices fraud.

D. Sanctions/penalties for cyber-related crimes
- The Computer Crime Act prescribes punishment ranging from a fine of 100,000 to 300,000 Sri Lanka rupees, and terms of imprisonment from six months to five years; or to both such fine and imprisonment for computer crimes.

E. National computer emergency response team (CERT)/computer security incident response team (CSIRT)
Sri Lanka Computer Emergency Readiness Team[733] is the national co-ordination point of contact for cybersecurity incidents and threats in Sri Lanka.[734]

F. National cybersecurity strategy
The Sri Lanka Information and Cybersecurity Strategy[735] is to be implemented for five years, between 2019 to 2023. It aims to: 'create a resilient and trusted cybersecurity ecosystem that will enable Sri Lankan citizens to realise the benefits of digital technology, and facilitate growth, prosperity and a better future for all Sri Lankans'.[736]

G. Initiatives to combat cybercrime
- Sri Lanka ratified the Convention on Cybercrime (ETS No. 185)[737] on 29 May 2015; it came into force on 1 September 2015.[738]
- Sri Lanka is one of the 195 INTERPOL [739] member countries.[740]
- Establishment of the national Computer Emergency Response Team and sectoral Computer Emergency Readiness Teams to respond to cyber threats and incidents.
- Creation of a Sri Lanka National Cyber Security Operation Centre (NCSOC)[741] with the aim: 'to drive a holistic and comprehensive approach to Cyber Security protection for the country'.[742] This will enable the country to identify cybersecurity attacks.

733 Sri Lanka Computer Emergency Readiness Team, available at: https://cert.gov.lk/ (accessed 17 January 2023).
734 Cybersecurity Act 2019, section 15(1), available at: www.cert.gov.lk/documents/Cyber%20Security%20Bill.pdf (accessed 16 January 2023).
735 National and Information Cybersecurity Strategy (2019–2023), available at: www.cert.gov.lk/documents/NCSStrategy.pdf (accessed 23 January 2023).
736 Ibid.
737 Council of Europe, 'The Budapest Convention (ETS No. 185) and is Protocols', available at: www.coe.int/en/web/cybercrime/the-budapest-convention (accessed 26 January 2023).
738 Council of Europe, 'Complete list of Council of Europe's treaties', Treaty Office, available at: www.coe.int/en/web/conventions/full-list (accessed 25 January 2023).
739 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
740 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).
741 ICTA (2017), Sri Lanka National Cyber Security Operation Center, 24 May, available at: www.icta.lk/ncsoc/ (accessed 31 January 2023).
742 Ibid.

- Continuous cybercrime training for law enforcement and judicial officers. Under the Sri Lanka Judges' Institute (SLJI), more than 200 judges were trained through the GLACY+ framework in 2019.[743]
- Participation in regional policy developments and collaborations. For instance, 'Sri Lanka took a leading role in the South–South collaboration effort by facilitating initial discussions between the Council of Europe and governmental representatives of Fiji, Ethiopia, Nepal and Papua New Guinea'.[744]
- Setting up a Digital Forensic Lab[745] and a Cyber Crime Unit (CCU) in the Sri Lanka Police[746] to investigate cyber allegations. There is also provision for e-report forms to be submitted through the police website.[747]

45. South Africa

A. National cyber threat landscape

According to the National Cyber Security Index (NCSI),[748] as of January 2023 South Africa ranked: 89th on the NCSI with a score of 36.36; 59th on the Global Cybersecurity Index; 92nd on the ICT Development Index; and 70th on the Networked Readiness Index.

B. National cybercrime legislation and related laws

- Cyber Crimes Act 2020 (CCA)[749]
- Electronic Transactions and Communications Act No. 25 of 2002 (ECTA)[750]
- The Regulation of Interception of Communications and Provision of Communication-related Information Act No. 70 of 2002 (RICA)[751]
- The Protection of Personal Information Act 4 of 2013 (POPI)[752]
- The Criminal Procedure Act No. 51 of 1977 (CPA)[753]

C. Scope/application of laws

- The CCA creates offences that have a bearing on cybercrime; and regulates the jurisdiction and powers to investigate cybercrimes. It also provides for some specific types of cybercrime, such as unlawful access, unlawful interception of data, unlawful interference with data or a computer program, cyber fraud, cyber forgery and uttering, and cyber extortion.

---

743 Council of Europe, 'GLACY+: Workshop on Cybercrime and e-Evidence for Sri Lankan New Judges', available at: www.coe.int/en/web/cybercrime/glacyplusactivities/-/asset_publisher/DD9qKA5QlKhC/content/glacy-workshop-on-cybercrime-and-e-evidence-for-sri-lankan-new-judges (accessed 30 January 2023).

744 South–South Cooperation Good Practices, available at: https://ecuador.unfpa.org/sites/default/files/pub-pdf/unfpa_good_practices_on_south-south_cooperation_2021.pdf (accessed 26 January 2023).

745 Digital Forensic Laboratory, available at: www.cert.gov.lk/1?lang=en&id=5 (accessed 25 January 2023).

746 Sri Lanka Security News, Online Edition of Daily News – Lakehouse Newspapers, available at: http://archives.dailynews.lk/2011/07/20/sec02.asp (accessed 30 January 2023).

747 Police Force, available at: www.police.lk/ (accessed 23 January 2023).

748 NCSI: South Africa, available at: https://ncsi.ega.ee/country/za/ (accessed 14 January 2023).

749 Cyber Crimes Act, available at: www.gov.za/sites/default/files/gcis_document/202106/44651gon324.pdf (accessed 13 January 2023).

750 South African Government, Electronic Communications and Transactions Act 25 of 2002, available at: www.gov.za/documents/electronic-communications-and-transactions-act (accessed 15 January 2023).

751 South African Government, Regulation of Interception of Communications and Provision of Communication-Related Information Act 70 of 2002, available at: www.gov.za/documents/regulation-interception-communications-and-provision-communication-related-information--13 (accessed 15 January 2023).

752 The Protection of Personal Information Act, available at: www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013protectionofpersonalinforcorrect.pdf (accessed 13 January 2023).

753 South African Government, Criminal Procedure Act 51 of 1977, sections 86 and 87, available at: www.gov.za/documents/criminal-procedure-act-1977-26-mar-2015-1224 (accessed 15 January 2023).

- The ECTA provides for the facilitation and regulation of electronic communications and transactions. Chapter XIII of the Act specifically addresses cybercrime, and offences such as unauthorised access to, interception of or interference with data, computer-related extortion, fraud, and forgery.[754]
- RICA aims at, among others, regulating the interception of certain communications, creation of offences and prescribing penalties for such offences.
- The CPA provides for the investigation and prosecution of crimes in the country.
- POPI provides for the protection of personal information processed, and the requirements for the processing of such personal information.

D. Sanctions/penalties for cyber-related crimes
- Part V of the CCA provides for sentencing. Section 19 thereof provides for liability on conviction to a fine or to imprisonment for a period not exceeding 5, 10 or 15 years or to both a fine and such imprisonment as applicable.
- Section 89 of the ECTA provides for penalties. It prescribes a fine or imprisonment for a period between 12 months and 5 years.

E. National computer emergency response team (CERT)/computer security incident response team (CSIRT)
- The Electronic Communications Security – Computer Security Incident Response Team (ECS-CSIRT)[755] serves as the South African government's security incident response team.
- The Cybersecurity Hub[756] is South Africa's national computer security incident response team (CSIRT).

F. National cybersecurity strategy
In 2012, the South African Cabinet adopted the National Cybersecurity Policy Framework (NCPF).[757] Its main objectives include to: 'facilitate the establishment of relevant structures in support of cybersecurity; ensure the reduction of cybersecurity threats and vulnerabilities; foster co-operation and co-ordination between government and private sector; promote and strengthen international co-operation; build capacity and promoting a culture of cybersecurity; and promote compliance with appropriate technical and operational cybersecurity standards'.[758]

G. Initiatives to combat cybercrime
- South Africa signed the Convention on Cybercrime (ETS No. 185)[759] on 23 November 2001. However, the signature has not been followed by ratification by the country.
- South Africa is one of the 195 INTERPOL [760] member countries.[761]
- The launch of a Cyber Security Fusion Centre. The national Cybersecurity Hub was also established in 2015. The hub brings together incident response teams and aids easy dissemination of cybersecurity information.

754 South African Government, Electronic Communications and Transactions Act 25 of 2002, available at: www.gov.za/documents/electronic-communications-and-transactions-act (accessed 15 January 2023).
755 Computer Security Incident Response Team, Electronic Communications Security, available at: www.first.org/members/teams/ecs-csirt (accessed 15 January 2023).
756 Cybersecurity Hub, available at: www.cybersecurityhub.gov.za/about-us (accessed 15 January 2023).
757 South African Government, National Cybersecurity Policy Framework, available at: www.gov.za/documents/national-cybersecurity-policy-framework-4-dec-2015-0000 (accessed 15 January 2023).
758 Ibid.
759 Council of Europe, 'The Budapest Convention (ETS No. 185) and is Protocols', available at: www.coe.int/en/web/cybercrime/the-budapest-convention (accessed 26 January 2023).
760 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
761 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).

- Putting in motion the development of a Cyber Warfare Strategy and a Cyberwarfare Implementation Plan to serve as a blueprint for strategic actions for combatting cybercrime.[762]

46. St Kitts and Nevis

A. National cyber threat landscape
According to the National Cyber Security Index (NCSI),[763] as of January 2023 St Kitts and Nevis ranked: 141st out of 161 countries on the NCSI with a score of 11.69; 153rd out of 194 countries on the Global Cybersecurity Index; and 37th on the ICT Development Index.

B. National cybercrime legislation and related laws
- Electronic Crimes Act 2009[764]
- Electronic Transactions Act 2011[765]

C. Scope/application of laws
- The Electronic Crimes Act prohibits unauthorised access to and abuse of computers and computer systems, as well as the information contained on those systems; and provides for related or incidental matters. Part II of the Act provides for electronic crimes such as illegal access and illegal remaining, interfering with data, interfering with computer a system, illegal interception, possession, sale, of illegal devices, computer-related fraud, unlawful disclosure of an access code, unauthorised access to a restricted computer system, child pornography, unlawful communications, computer-related forgery, data espionage, identity-related crimes, and spam.[766]
- The Electronic Transactions Act establishes the legal principles applicable to the conduct of electronic commerce and the processing, verification and attribution of electronic records; and provides for the approval, registration and liabilities of service providers and for incidental and connected purposes.

D. Sanctions/penalties for cyber-related crimes
- A person who is convicted of an offence under the Electronic Crimes Act shall be liable to a fine between EC$5,000 to 100,000 Eastern Caribbean dollars, or to imprisonment for a term ranging from one to seven years, or both fine and imprisonment. In the case of a corporation guilty of child pornography, liability shall be to a fine of 250,000 dollars.

E. National computer emergency response team (CERT)/computer security incident response team (CSIRT)
St Kitts and Nevis does not currently have an officially recognised CERT.

F. National cybersecurity strategy
St Kitts and Nevis does not currently have an officially designated national cybersecurity strategy. However, the National Security Strategy[767] of the Ministry of National Security lists cybercrime under the threat assessment areas.

---

762 Sutherland, E (2017), 'Governance of Cybersecurity – The Case of South Africa', *The African Journal of Information and Communication* 20, p.83, available at: http://www.scielo.org.za/scielo.php?script=sci_abstract&pid=S2077-72132017000100005&lng=en&nrm=iso&tlng=en (accessed 30 January 2023).
763 NCSI: St Kitts and Nevis, available at: https://ncsi.ega.ee/country/kn/ (accessed 14 January 2023).
764 Electronic Crimes Act, available at: https://aglcskn.info/wp-content/documents/Act17TOC/Ch-04_41-Electronic-Crimes-Act.pdf (accessed 16 January 2023).
765 Electronic Transactions Act, available at: https://skncustoms.com/pdfs/GoSKN-ElectronicTransactionsAct2011.pdf (accessed 16 January 2023).
766 Electronic Crimes Act, sections 5-17, available at: https://aglcskn.info/wp-content/documents/Act17TOC/Ch-04_41-Electronic-Crimes-Act.pdf (accessed 16 January 2023).
767 Ministry of National Security, National Security Strategy of St Kitts and Nevis, available at: https://www.sknis.gov.kn/wp-content/uploads/2021/02/NATIONAL-SECURITY-STRATEGY_JANUARY-2021.pdf

G. Initiatives to combat cybercrime

- St Kitts and Nevis is a member of the Caribbean Community (CARICOM), which focuses on integration and co-operation in areas such as trade, criminal justice, the environment and technical standards among its member states.[768]
- St Kitts and Nevis one of the 195 INTERPOL [769] member countries.[770]
- Collaboration and co-operation with international organisations such as OAS,[771] CARICOM Implementation Agency for Crime and Security (IMPACS),[772] and agencies like the Federal Bureau of Investigation (FBI).[773]
- Implementation of the National Crime Reduction and Prevention Strategy (2017),[774] which reflects the community's perception of crime and develops strategies to curb those crimes.
- The National ICT Strategic Plan[775] proposes the establishment of an ICT Crimes Unit (ICTCU) to deal with computer-related crimes.[776] Also proposed is the creation of a Cyber Crime Unit in the country's police force.
- The Prime Minister and Minister of National Security, on 30 January 2023[777] in a press briefing, made assurances of the government's commitment to putting crime reduction initiatives in place. Already in existence are initiatives such as the Teen and Police Service initiative (TAP)[778] and Mentoring, Advising, Guiding, and Instructing Children (MAGIC), which targets school children and addresses issues such as bullying and cyber interference.[779]

47. St Vincent and The Grenadines

A. National cyber threat landscape

According to the National Cyber Security Index (NCSI),[780] as of January 2023 St Vincent and the Grenadines ranked: 153rd out of 161 countries on the NCSI with a score of 7.79; 154th out of 194 countries on the Global Cybersecurity Index; and 82nd on the ICT Development Index.

B. National cybercrime legislation and related laws

- Cyber Crimes Act 2016[781]

768 PublicTechnology.net (2022), 'No one is an island: how Caribbean states are working together to tackle cybercrime', 17 October, available at: https://publictechnology.net/articles/features/no-one-island-how-caribbean-states-are-working-together-tackle-cybercrime (accessed 24 January 2023).
769 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
770 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).
771 OAS (2009), 'OAS – Organization of American States: Democracy for Peace, Security, and Development', 1 August, available at: www.oas.org/en/ (accessed 31 January 2023).
772 CARICOM Implementation Agency for Crime and Security, available at: https://caricomimpacs.org/about-us-v1/ (accessed 27 January 2023).
773 Federal Bureau of Investigation, Cyber Crime, available at: www.fbi.gov/investigate/cyber (accessed 31 January 2023).
774 SKNIS (2017), National Crime Reduction and Prevention Strategy, 30 May, available at: www.sknis.gov.kn/2017/05/30/national-crime-reduction-and-prevention-strategy/ (accessed 31 January 2023).
775 National ICT Strategic Plan, available at: https://unstats.un.org/unsd/dnss/docViewer.aspx?docID=2297 (accessed 16 January 2023).
776 Ibid.
777 ZIZ Online (2023), 'Several crime reduction initiatives to be implemented in St Kitts And Nevis', 30 January, available at: https://zizonline.com/several-crime-reduction-initiatives-to-be-implemented-in-st-kitts-and-nevis/ (accessed 26 January 2023).
778 *NevisPages.com* (2014), 'TAPS – Teen and Police Service, The Newest Teen Intervention Initiative By The Police', 6 July, available at: www.nevispages.com/taps-teen-and-police-service-the-newest-teen-intervention-initiative-by-the-police/ (accessed 31 January 2023).
779 SKNVibes, 'Education Ministry Gives Full Support to M.A.G.I.C.', available at: www.sknvibes.com/news/newsdetails.cfm/86860 (accessed 31 January 2023).
780 NCSI: St Vincent and the Grenadines, available at: https://ncsi.ega.ee/country/vc/ (accessed 14 January 2023).
781 Cyber Crimes Act, available at: www.assembly.gov.vc/assembly/images/stories/cybercrime%20bill%202016.pdf (accessed 15 January 2023).

- Electronic Transactions Act (ETA) 2007[782]
- Electronic Evidence Act 2004

C. Scope/application of laws

- The Cyber Crimes Act provides for the creation of offences related to cybercrimes and for related matters. Part II thereof provides for cyber offences such as illegal access to a computer system, illegally remaining in a computer system, illegal interception, illegal data interference, illegal acquisition of data, illegal system interference, offences affecting critical infrastructure, illegal devices, identity-related crimes, computer-related forgery, computer-related fraud, child pornography, harassment utilising means of electronic communication, spam and spoofing.[783]
- The Electronic Transactions Act provides for the facilitation and regulation of electronic communications and transactions, to prevent abuse of information systems and to provide for matters connected therewith. Part X of the Act provides for information systems and computer-related crimes such as illegal access, interfering with data, interfering with an information system, illegal interception of data, illegal devices, child pornography, electronic fraud and cyber stalking.[784]
- The Electronic Evidence Act provides for the legal recognition of electronic records, admissibility in legal proceedings of evidence generated by computers or other similar devices; and for matters connected therewith.

D. Sanctions/penalties for cyber-related crimes

- The Cyber Crimes Act provides for sanctions ranging from a fine of EC$10,000 to 1 million Eastern Caribbean dollars, and imprisonment from 3 to 15 years, or both fine and imprisonment.
- The Electronic Transactions Act provides for sanctions ranging from a fine of EC$5,000 to 30,000 dollars Eastern Caribbean, and imprisonment from 1 to 10 years, or both fine and imprisonment.

E. National computer emergency response team (CERT)/computer security incident response team (CSIRT)

At the time of report writing, there was no available information regarding any officially recognised national CERT in St Vincent and the Grenadines.

F. National cybersecurity strategy

At the time of writing, there was no available information on an official national cybersecurity strategy for St Vincent and the Grenadines.

G. Initiatives to combat cybercrime

- St Vincent and the Grenadines is a member of the Caribbean Community (CARICOM). Therefore, through the operation of the CARICOM Implementation Agency for Crime and Security (IMPACS), it benefits from CARICOM's cybersecurity efforts and strategies.
- St Vincent and the Grenadines is one of the 195 INTERPOL [785] member countries.[786]

782 Electronic Transactions Act, available at: http://www.oas.org/juridico/spanish/cyb_svg_electronic_act_2007.pdf (accessed 16 January 2023).
783 Electronic Crimes Bill, sections 3–18, available at: www.assembly.gov.vc/assembly/images/stories/cybercrime%20bill%202016.pdf (accessed 15 January 2023).
784 Electronic Transactions Act, sections 66–73, available at: www.oas.org/juridico/spanish/cyb_svg_electronic_act_2007.pdf (accessed 16 January 2023).
785 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
786 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).

48. Tanzania

A. National cyber threat landscape

According to the National Cyber Security Index (NCSI),[787] as of January 2023 Tanzania ranked: 108th on the NCSI with a score of 24.68; 37th on the Global Cybersecurity Index; 165th on the ICT Development Index; and 107th on the Networked Readiness Index.

B. National cybercrime legislation and related laws

- The Cybercrimes Act 2015[788]
- Tanzania Electronic and Postal Communications Act 2010[789]
- The Tanzania Electronic and Postal Communications (Computer Emergency Response Team) Regulations 2011[790]

C. Scope/application of laws

- The Cybercrimes Act makes provision for criminalising offences related to computer systems and information communication technologies; and provides for the investigation, collection and use of electronic evidence. PART II of the Act makes provisions relating to offences and penalties. It includes offences such as illegal access, data espionage, illegal system interference, computer-related forgery and fraud, pornography and child pornography, identity-related crimes, and cyber bullying.
- The Electronic and Postal Communications Act provides for electronic and telecommunications law, with a view to keeping abreast of developments in the industry. Part VI of the Act provides for offences and penalties. Offences relating to electronic communications include transmission of obscene communication, interception of communications, fraudulent use of network facilities and services, interference of transmission of electronic communications, and unauthorised access or use of a computer system.

D. National computer emergency response team (CERT)/computer security incident response team (CSIRT)

Tanzania Computer Emergency Response Team[791] was established under section 124 of the Electronic and Postal Communications Act 2010.[792] It is responsible for co-ordinating and responding to cybersecurity incidents in the country.[793]

F. National cybersecurity strategy

At the time of writing, there was no available information of an officially designated national cybersecurity strategy for Tanzania.

G. Initiatives to combat cybercrime

- Tanzania is one of the 195 INTERPOL[794] member countries.[795]
- Establishment of a Cyber Crime Unit under the police force to investigate cybercrime and prosecute cyber offenders.

787 NCSI: Tanzania, available at: https://ncsi.ega.ee/country/tz/ (accessed 14 January 2023).
788 Principal Legislation, Cybercrimes Act, available at: www.tanzanialaws.com/principal-legislation/cybercrimes-act (accessed 15 January 2023).
789 ICT Policy Africa, Tanzania Electronic and Postal Communications Act 2010, p.1, available at: https://ictpolicyafrica.org/es/document/a75omimq6wr (accessed 15 January 2023).
790 ICT Policy Africa, Tanzania Electronic and Postal Communications (Computer Emergency Response Team) Regulations, 2011, p.1, available at: https://ictpolicyafrica.org/es/document/q4coyg0yg4 (accessed 15 January 2023).
791 Tanzania Computer Emergency Response Team, available at: www.tzcert.go.tz/ (accessed 15 January 2023).
792 ICT Policy Africa, Tanzania Electronic and Postal Communications Act 2010, p.1, available at: https://ictpolicyafrica.org/es/document/a75omimq6wr (accessed 15 January 2023).
793 Tanzania Computer Emergency Response Team, available at: www.tzcert.go.tz/ (accessed 15 January 2023).
794 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
795 Interpol member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).

- Establishment of a permanent national committee to oversee and 'address challenges of cyber bullying, controlling fraud and cyber theft through mobile phones in the country'.[796]
- International collaboration and co-operation on fighting cybercrime, and facilitation of awareness-raising programmes to empower the public.[797]

49. Togo

A. National cyber threat landscape
There is no cyber threat landscape assessment rating for Togo on the National Cyber Security Index (NCSI).

B. National cybercrime legislation and related laws
- Law on Cybersecurity and the Fight against Cybercrime (*Loi N° 2018 – 026 du 07/12/18 sur la cybersécurité et la ute contre la cybercriminalité*)[798]
- Law on Electronic Transactions [799]

C. Scope/application of laws
- The Law on Cybersecurity and the Fight against Cybercrime is the substantive law on cybercrime in the country. It covers offences such as illegal access, data and interference, as well as offences of child pornography.

D. National computer emergency response team (CERT)/computer security incident response team (CSIRT)
Togo Computer Emergency Response Team (CERT.tg)[800] is responsible for ensuring monitoring and response to cyber incidents in the country.

E. National cybersecurity strategy
At the time of writing, there was no available information of an officially designated national cybersecurity strategy for Togo.

F. Initiatives to combat cybercrime
- Togo is one of the 195 INTERPOL [801] member countries.[802]
- Launch of the CERT.tg, which provides 'round-the-clock' monitoring and response to cyber incidents in the country.
- Facilitation of cybersecurity training sessions for law enforcement and security personnel. Courses and trainings are also organised for government officials and individuals through the CERT.tg.[803]
- Commencement of a plan to set up an African Centre for Coordination and Research in Cybersecurity, based in the capital city Lomé. This will serve as a regional hub for cybersecurity information and intelligence.
- The Government of Togo hosted the First African Heads of States Cybersecurity Summit in conjunction the United Nations Economic Commission for Africa (UNECA) in March 2022.

796 CIO Africa (2021), 'Tanzanian Government Outlines Measures To Curb Cybercrime', 13 September, available at: https://cioafrica.co/tanzanian-government-outlines-measures-to-curb-cybercrime/ (accessed 30 January 2023).
797 Mwalongo, S (2022), 'Tanzania: Govt touts cooperation in cybercrime fight', *Tanzania Daily News*, Dar es Salaam, 27 February, available at: https://allafrica.com/stories/202202270005.html (accessed 30 January 2023).
798 Loi N° 2018 – 026 du 07/12/18 *sur la cybersécurité et la lutte contre la cybercriminalité*, available at: https://jo.gouv.tg/sites/default/files/JO/JOS_07_12_2018-63E%20ANNEE%20N%C2%B024TER.pdf#page=1 (accessed 13 January 2023).
799 Loi N° 2017 – 07 *transactions electroniques*, available at: www.droit-afrique.com/uploads/Togo-Loi-2017-07-transactions-electroniques.pdf (accessed 13 January 2023).
800 CERT.TG – La Protection Du Cyberespace Togolais, available at: https://cert.tg/ (accessed 15 January 2023).
801 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
802 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).
803 CERT.TG – La Protection Du Cyberespace Togolais, available at: https://cert.tg/ (accessed 15 January 2023).

It was held in Lomé, to discuss effective and efficient measures to prioritise cybersecurity in the region. This led to the signing of the Lomé Declaration on Cybersecurity and Fight Against Cybercrime 2022. The Declaration voices a commitment to establish a framework to promote a cybersecurity culture in Africa. The Declaration was signed by Heads and representatives of African governments.

- Togo has entered into a partnership agreement with the UNECA to establish the first African Centre for Coordination and Research in Cybersecurity (ACCRC).
- Various regional and international co-operation on combatting cybercrime, such as collaboration between different African countries in implementing the Lomé Declaration to broaden the legal and regulatory framework; signing of a memorandum of understanding (MOU) to establish the Cybersecurity Centre. Togo has ratified the African Union Convention on Cybersecurity and Personal Data Protection ('the Malabo Convention') 2014.

50. Tonga

A. National cyber threat landscape
According to the National Cyber Security Index (NCSI),[804] as of January 2023 Tonga ranked: 112th out of 161 countries on the NCSI with a score of 23.38; 128th out of 194 countries on the Global Cybersecurity Index; and 110th on the ICT Development Index.

B. National cybercrime legislation and related laws
- Computer Crimes Act 2003[805]

C. Scope/application of laws
- The Computer Crimes Act was enacted to combat computer crime and to provide for the collection and use of electronic evidence. Part II of the Act provides for cyber offences such as illegal access,[806] interfering with data,[807] interfering with a computer system,[808] illegal interception of data,[809] and illegal devices.[810]

D. Sanctions/penalties for cyber-related crimes
- The Computer Crimes Act provides for penalties ranging from a fine between T$5,000 and 100,000 Tongan dollars, or imprisonment between 1 and 20 years.

E. National computer emergency response team (CERT)/computer security incident response team (CSIRT)
Tonga CERT[811] began operating on 1 July 2016 and is tasked with ensuring a co-ordinated response to cyber incidents in the country.

F. National cybersecurity strategy
At the time of writing, there was no available information of an officially designated national cybersecurity strategy for Tonga. There is a Tonga *Cybersecurity Manual*, which was developed to provide strategic and practical guidance on how organisations in Tonga can mitigate cyber threats and cyberattacks. The manual is not a national cybersecurity strategy.

804 NCSI: Tonga, available at: https://ncsi.ega.ee/country/to/ (accessed 14 January 2023).
805 Computer Crimes Act, available at: https://ago.gov.to/cms/images/LEGISLATION/PRINCIPAL/2003/2003-0014/ComputerCrimesAct_3.pdf (accessed 16 January 2023).
806 Ibid, section 4.
807 Ibid, section 5.
808 Ibid, section 6.
809 Ibid, section 7.
810 Ibid, section 8.
811 cert.gov.to, CERT Tonga, available at: www.cert.gov.to/ (accessed 31 January 2023).

G. Initiatives to combat cybercrime

- Tonga ratified the Convention on Cybercrime (ETS No. 185)[812] on 9 May 2017; it came into force on 1 September 2017.[813]
- Tonga is one of the 195 INTERPOL [814] member countries.[815]
- Formulation of policies such as the ICT Policy,[816] which established the Cyber Challenges Task Force (CCTF) on 13 December 2013, to provide strategic and co-ordinated responses to cyber and technological challenges in the country.
- Creation of the Transnational Crime Unit (TCU) in the Tonga police force in 2003, which became the Serious Organized Transnational Crime Unit (SOTCU)[817] in 2010. It is tasked with responding to and investigating transnational crimes, including cybercrimes.
- International co-operation and participation in regional outreaches. For instance, the Pacific Islands Law Officers Network Regional Forum was held in Tonga in 2018, with cybercrime as the theme.[818]

51. Trinidad and Tobago

A. National cyber threat landscape

According to the National Cyber Security Index (NCSI),[819] as of January 2023 Trinidad and Tobago ranked: 94thout of 161 countries on the NCSI with a score of 33.77; 125th out of 194 countries on the Global Cybersecurity Index; 68th on the ICT Development Index; and 85th on the Networked Readiness Index.

B. National cybercrime legislation and related laws

- Computer Misuse Act 2000[820]
- Electronic Transactions Act, No. 6 of 2011[821]

C. Scope/application of laws

- The Computer Misuse Act prohibits any unauthorised access, use or interference with a computer, and for other related matters. Part II of the Act provides for computer offences such as unauthorised access to a computer program or data,[822] access with intent to commit or facilitate commission of offence,[823] unauthorised modification of a computer program or data,[824] unauthorised use or interception of a computer service,[825] unauthorised

812 Council of Europe, 'The Budapest Convention (ETS No. 185) and is Protocols', available at: www.coe.int/en/web/cybercrime/the-budapest-convention (accessed 26 January 2023).
813 Council of Europe, 'Complete list of Council of Europe's treaties', Treaty Office, available at: www.coe.int/en/web/conventions/full-list (accessed 25 January 2023).
814 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
815 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).
816 ICT Policy, available at: http://pippr.victoria.ac.nz/bitstream/handle/123456789/27/Tonga%20-%20national%20ICT%20policy.pdf?sequence=1 (accessed 7 January 2023).
817 Serious Organised Transitional Crime Unit, available at: https://nautilus.org/publications/books/australian-forces-abroad/tonga/transnational-crime-unit-tonga/ (accessed 7 January 2023).
818 'Cybersecurity and Safeguarding Electronic Transactions in the Pacific Islands', Policy Brief available at: https://theprif.org/sites/default/files/documents/policy_brief_cyber_security_low_res_rev4.pdf (accessed 23 January 2023).
819 NCSI: Trinidad and Tobago, available at: https://ncsi.ega.ee/country/tt/ (accessed 14 January 2023).
820 Computer Misuse Act 2000, available at: https://rgd.legalaffairs.gov.tt/Laws2/Alphabetical_List/lawspdfs/11.17.pdf (accessed 15 January 2023).
821 Electronic Transactions Act, available at: https://rgd.legalaffairs.gov.tt/Laws2/Alphabetical_List/lawspdfs/22.05.pdf (accessed 16 January 2023).
822 Computer Misuse Act 2000, section 3, available at: https://rgd.legalaffairs.gov.tt/Laws2/Alphabetical_List/lawspdfs/11.17.pdf (accessed 15 January 2023).
823 Ibid, section 4.
824 Ibid, section 5.
825 Ibid, section 6.

obstruction of or use of a computer,[826] unauthorised disclosure of an access code,[827] unauthorised receiving or giving access to a computer program or data,[828] and causing a computer to cease to function.[829]

- The Electronic Transactions Act gives legal effect to electronic documents, electronic records, electronic signatures and electronic transactions.

D. Sanctions/penalties for cyber-related crimes
The Computer Misuse Act provides penalty ranging from a fine of TT$15,000 to 50,000 Trinidad and Tobago dollars and imprisonment between two and five years.

E. National computer emergency response team (CERT)/computer security incident response team (CSIRT)
Trinidad and Tobago Cyber Security Incident Response Team (TT-CSIRT)[830] is tasked with responding to cyber threats and securing the country's digital infrastructure.

F. National cybersecurity strategy
The National Cybersecurity Strategy[831] seeks to guide all operations and initiatives relating to cybersecurity in Trinidad and Tobago. Its main objective is to provide a governance framework for all cybersecurity matters, by identifying the requisite organisational and administrative structures necessary to address and respond to cyber threats. [832]

G. Initiatives to combat cybercrime
- Trinidad and Tobago is a member of the Caribbean Community (CARICOM) and therefore receives support from IMPACS in addressing cyberthreats and vulnerabilities. As a member state, Trinidad and Tobago also signed off on the CARICOM Cyber Security and Cybercrime Action Plan (CCSCAP).
- Trinidad and Tobago is one of the 195 INTERPOL [833] member countries.[834]
- Formulation of a National ICT Plan[835] and the Policy Framework for Sustainable Development, which both state the importance of a cybersecurity framework.
- International collaboration and co-operation on cybersecurity with institutions such as: the Organization of American States (OAS),[836] the EU, the Caribbean Telecommunications Union (CTU)[837] and the International Telecommunication Union (ITU).[838]
- The Trinidad and Tobago Cyber Security Agency (TTCSA), which is responsible for the co-ordination, implementation and monitoring of cybersecurity programmes in Trinidad and Tobago, has been engaged in continuous improvement and governance of cyber security initiatives in the country.[839]

826 Ibid, section 7.
827 Ibid, section 8.
828 Ibid, section 10.
829 Ibid, section 11.
830 TT-CSIRT: Trinidad and Tobago Cyber Security Incident Response Team, Securing the Nation's Digital Infrastructure, available at: https://ttcsirt.gov.tt/ (accessed 1 February 2023).
831 National Cybersecurity Strategy , available at: www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/TrinidadandTobagoNationalCyberSecurityStategyEnglish.pdf (accessed 23 January 2023).
832 Ibid.
833 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
834 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).
835 National ICT Plan, available at: https://mpa.gov.tt/sites/default/files/file_upload/publications/NICT%20Plan%202018-2022%20-%20August%202018.pdf (accessed 13 January 2023).
836 OAS (2009), 'OAS – Organization of American States: Democracy for Peace, Security, and Development', 1 August, available at: www.oas.org/en/ (accessed 31 January 2023).
837 Caribbean Telecommunications Union – Shaping Caribbean Telecommunications, available at: https://ctu.int/ (accessed 1 February 2023).
838 ITU, 'ITU: Committed to Connecting the World', available at: www.itu.int:443/en/Pages/default.aspx (accessed 1 February 2023)
839 National Cybersecurity Strategy, available at: www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/TrinidadandTobagoNationalCyberSecurityStategyEnglish.pdf (accessed 23 January 2023).

52. Tuvalu

A. National cyber threat landscape
According to the National Cyber Security Index (NCSI),[840] as of January 2023 Tuvalu ranked: 160th out of 161 countries on the NCSI with a score of 2.60; and 168th out of 194 countries on the Global Cybersecurity Index.

B. State of cybercrime laws
There is no comprehensive or specific cybercrime law in Tuvalu. The existing related laws include the Counter Terrorism and Transnational Organised Crime Ac 2009,[841] the Mutual Assistance in Criminal Matters Act, the Proceeds of Crime Act and the Extradition Act. Further, it has been reported that a Cybercrime Bill might be in development.[842]

C. National computer emergency response team (CERT)/computer security incident response team (CSIRT)
There is no record of a national CERT in Tuvalu.

D. National cybersecurity strategy
At the time of writing, there was no available information on an officially designated national cybersecurity strategy for Tuvalu.

E. Initiatives to combat cybercrime
There exist co-ordinated efforts to combat transnational crime and share related information. Some of these include efforts by the 'Tuvaluan Combined Law Enforcement Agency Group (CLAG) which works to co-ordinate information sharing'[843]. Regional efforts also include mechanisms to respond to transnational and border threats, such as the Pacific Transnational Crime Coordination Centre[844] and the Biketawa and Boe Declarations.[845]

53. Uganda

A. National cyber threat landscape
According to the National Cyber Security Index (NCSI),[846] as of January 2023 Uganda ranked: 61st on the NCSI with a score of 54.55; 72nd on the Global Cybersecurity Index; 152nd on the ICT Development Index; and 116th on the Networked Readiness Index.

B. National cybercrime legislation and related laws
- Computer Misuse Act 2011(CMU)[847]
- Computer Misuse (Amendment) Act 2022[848]

840 NCSI: Tuvalu, available at: https://ncsi.ega.ee/country/tv/ (accessed 14 January 2023).
841 Counter Terrorism and Transnational Organised Crime Act 2009, available at: http://tuvalu-legislation.tv/cms/images/LEGISLATION/PRINCIPAL/2009/2009-0006/CounterTerrorismandTransnationalOrganisedCrimeAct2009_1.pdf (accessed 12 January 2023).
842 Department of Foreign Affairs (2022), Transnational Crime and Border Security, 16 May, available at: https://dfa.gov.tv/index.php/transnational-crime-and-border-security/ (accessed 31 January 2023).
843 Ibid.
844 Pacific Transnational Crime Network (PICP), available at: https://picp.co.nz/our-work/pacific-transnational-crime-network/ (accessed 31 January 2023).
845 Forum Sec, Boe Declaration on Regional Security, available at: www.forumsec.org/2018/09/05/boe-declaration-on-regional-security/ (accessed 31 January 2023).
846 NCSI: Uganda, available at: https://ncsi.ega.ee/country/ug/ (accessed 14 January 2023).
847 Ministry of ICT & National Guidance, The Computer Misuse Act 2011, available at: https://ict.go.ug/2019/12/03/the-computer-misuse-act-2011/ (accessed 15 January 2023).
848 Computer Misuse (Amendment) Act 2022, available at: https://chapterfouruganda.org/sites/default/files/downloads/The-Computer-Misuse-%28Amendment%29-Act-2022.pdf (accessed 13 January 2023).

C. Scope/application of laws
- The CMU 2011 makes provision for the safety and security of electronic transactions and information systems; and prevents the unlawful access, abuse or misuse of information systems, including computers. Part IV of the Act provides for computer misuse offences such as unauthorised access, unauthorised modification of computer material, unauthorised use or interception of a computer service, unauthorised disclosure of information, electronic fraud, child pornography, cyber harassment and cyber stalking.[849]
- The CMU (Amendment) Act amends the Computer Misuse Act 2011 and enhances its provisions on: authorised access to information or data; prohibition of unlawful sharing of information relating to a child; the sending or sharing of malicious or unsolicited information; and for other related matters.

D. National computer emergency response team (CERT)/computer security incident response team (CSIRT)
The Uganda Computer Emergency Response Team (NITA-U) is also known as the Uganda National Computer Emergency Response Team and Coordination Center (Cert.Ug/Cc).[850]

E. National cybersecurity strategy
The National Cybersecurity Strategy 2022–2026[851] discusses measures and strategic principles to combat cybercrime and ensure security of the country's cyberspace.

F. Initiatives to combat cybercrime
- Uganda is one of the 195 INTERPOL [852] member countries.[853]
- Establishment of the Electronic Counter Measure Unit (ECMU) within the Uganda Police Force. The unit is responsible for investigating internet- and computer-related crimes.
- The drafting of a National Cybersecurity Strategy,[854] which discusses measures and strategic principles to combat cybercrime and ensure security of the country's cyberspace.
- Presence of a CERT,[855] which ensures timely monitoring of and response to cyber incidents in the country.

54. United Kingdom

A. National cyber threat landscape
According to the National Cyber Security Index (NCSI),[856] as of January 2023 the United Kingdom ranked: 22nd out of 161 countries on the NCSI with a score of 77.92; 2nd out of 194 countries on the Global Cybersecurity Index; 5th on the ICT Development Index; and 10th on the Networked Readiness Index.

B. National cybercrime legislation and related laws
- Computer Misuse Act 1990 (as amended)[857]
- Electronic Communications Act 2000[858]

849 Ministry of ICT & National Guidance, The Computer Misuse Act 2011, sections 12–25, available at: https://ict.go.ug/2019/12/03/the-computer-misuse-act-2011/ (accessed 15 January 2023).
850 Uganda Computer Emergency Response Team, available at: https://cert.ug/ (accessed 13 January 2023).
851 National Cybersecurity Strategy, available at: https://ega.ee/wp-content/uploads/2022/08/Ugandan-national-cybersecurity-strategy.pdf (accessed 23 January 2023).
852 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
853 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).
854 National Cybersecurity Strategy, available at: https://ict.go.ug/wp-content/uploads/2021/08/Draft_National_Cybersecurity_Strategy_Ug_v1.pdf (accessed 23 January 2023).
855 Uganda Computer Emergency Response Team, available at: https://cert.ug/ (accessed 13 January 2023).
856 NCSI: United Kingdom, available at: https://ncsi.ega.ee/country/uk/ (accessed 14 January 2023).
857 Computer Misuse Act 1990, available at: www.legislation.gov.uk/ukpga/1990/18/contents (accessed 19 January 2023).
858 Electronic Communications Act 2000, available at: www.legislation.gov.uk/ukpga/2000/7/contents (accessed 19 January 2023).

- Communications Act 2003[859]
- Network and Information Systems Regulations 2018[860]

C. Scope/application of laws
- The Computer Misuse Act makes provision for securing computer material against unauthorised access or modification, and for connected purposes. It provides for cyber offences such as unauthorised access to computer material, unauthorised access with intent to commit or facilitate commission of further offences, unauthorised acts with intent to impair, or with recklessness as to impairing, operation of a computer, and unauthorised acts causing, or creating risk of, serious damage.
- The Electronic Communications Act makes provision to facilitate the use of electronic communications and electronic data storage.

D. Sanctions/penalties for cyber-related crimes
- The Computer Misuse Act prescribes a range of penalties for a person guilty of an offence under it. It prescribes imprisonment between 12 months to 14 years, or to a fine not exceeding the statutory maximum, or to both a fine and imprisonment. However, where the offence creates a significant risk of serious damage to human welfare or national security, 'a person guilty of the offence is liable, on conviction on indictment, to imprisonment for life, or to a fine, or to both'.[861]

E. National computer emergency response team (CERT)/computer security incident response team (CSIRT)
CERT-UK is the UK's national computer emergency response team. The country also has a National Cyber Security Centre (NCSC).

F. National cybersecurity strategy
- The National Cyber Security Strategy 2022[862] sets out the government's vision for the future of cyberspace as ensuring that 'citizens, business and government can enjoy the full benefits of a safe, secure and resilient cyberspace through working together to enhance the UK's overall security and resilience'.[863] The new strategy builds on the National Cyber Security Strategy 2016–2021.
- The UK also has the Home Office Cyber Crime Strategy[864] through which the Home Office works closely with the Office of Cyber Security towards developing policies to counter cybercrime and its impact on UK. The Cybercrime Strategy was developed in response to the need for the UK to develop an integrated approach to tackling the threats from the internet and associated technology therefore it was seen as an imperative that the UK should develop a strategy for dealing with cybercrime. To ensure that the Cyber Crime Strategy continues to evolve and keep pace with changing threats the strategy is reviewed on a six-monthly basis to ensure consistency with the UK National Security Strategy[865] and the UK Cyber Security Strategy.

---

859 Communications Act 2003, available at: www.legislation.gov.uk/ukpga/2003/21/contents (accessed 19 January 2023).
860 The Network and Information Systems Regulations 2018, available at: www.legislation.gov.uk/uksi/2018/506 (accessed 19 January 2023).
861 Computer Misuse Act 1990, section 3Za, available at: www.legislation.gov.uk/ukpga/1990/18/contents (accessed 19 January 2023).
862 Government of the UK, Government Cyber Security Strategy: 2022 to 2030, available at: www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030 (accessed 19 January 2023).
863 Ibid.
864 Cybercrime Strategy, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228826/7842.pdf (accessed 23 January 2023).
865 National Security Strategy, available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228539/7291.pdf (accessed 27 January 2023).

G. Initiatives to combat cybercrime

- The UK is one of the 195 INTERPOL [866] member countries.[867]
- The UK is a party to the Council of Europe Convention on Cybercrime (ETS No. 185) 2001 entered into force in the United Kingdom on 1 September 2011.
- Active commitment to ensuring law enforcement agencies combat cybercrimes. This is done through establishment of agencies such as the National Crime Agency[868], e-Crime Unit, the Police Central e-crime Unit (PCeU), and the Child Exploitation and Online Protection (CEOP) Centre.[869]
- Establishment of the National Cyber Security Centre (NCSC)[870] to provide strategic leadership across government.
- Establishment of the UK Council for Internet Safety (UKCIS)[871] to ensure a co-ordinated approach towards protection of users online.
- Creation of the 'Action Fraud'[872] initiative with the UK National Fraud Intelligence Bureau (NFIB) and the National Fraud Authority (NFA) to tackle the most serious and harmful threats, while improving the country's capability to prevent such threats.[873]
- Signing up for the Cyber Security Information Sharing Partnership (CiSP) initiative, which engages stakeholders and provides warnings and analysis of cyber threats.[874]
- Creation of the Cyber Essentials Scheme[875] to help organisations mitigate the risk to their IT systems from online threats.
- Establishment of the National Cyber Force (NCF) to develop offensive cyber capabilities.
- Development of an integrated National Crime Agency (NCA)-led national law enforcement response.
- Establishment of the UK Internet Watch Foundation (IWF)[876] by the internet industry in 1996. The IWF serves as 'the UK Hotline for reporting child sexual abuse content hosted worldwide and criminally obscene and incitement to racial hatred content hosted in the UK'.[877]

55. Vanuatu

A. National cyber threat landscape
According to the National Cyber Security Index (NCSI),[878]

866 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
867 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).
868 National Crime Agency, Home, available at: www.nationalcrimeagency.gov.uk/ (accessed 31 January 2023).
869 CEOP Safety Centre, available at: www.ceop.police.uk/Safety-Centre/ (accessed 23 January 2023).
870 NCSC, available at: www.ncsc.gov.uk/ (accessed 31 January 2023).
871 Government of the UK, UK Council for Internet Safety, available at: www.gov.uk/government/organisations/uk-council-for-internet-safety (accessed 31 January 2023).
872 Action Fraud, available at: https://actionfraud.police.uk/ (accessed 27 January 2023).
873 Government of the UK, Government Cyber Security Strategy: 2022 to 2030, available at: www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030 (accessed 19 January 2023).
874 Cyber Security Information Sharing Partnership (CiSP), available at: www.ncsc.gov.uk/information/cyber-security-information-sharing-partnership--cisp- (accessed 31 January 2023).
875 Government of the UK, Cyber Essentials Scheme: Overview, available at: www.gov.uk/government/publications/cyber-essentials-scheme-overview (accessed 19 January 2023).
876 The Internet Watch Foundation – Eliminating Child Sexual Abuse Online, available at: www.iwf.org.uk/ (accessed 31 January 2023).
877 Government of the UK, Government Cyber Security Strategy: 2022 to 2030, available at: www.gov.uk/government/publications/government-cyber-security-strategy-2022-to-2030 (accessed 19 January 2023).
878 NCSI: Vanuatu, available at: https://ncsi.ega.ee/country/vu/ (accessed 14 January 2023).

B. National cybercrime legislation and related laws
- Cybercrime Act No. 22 of 2021[879]
- Electronic Transactions Act 2000[880]

C. Scope/application of laws
- The Cybercrime Act 2021 enables action against threats such as cyberbullying, stalking and digital hate crimes, while providing important protections for free speech, the public good, and identity protection. The Act also sets out clear terms for how data can be shared between jurisdictions.
- The Electronic Transactions Act makes provision for electronic transactions and for related matters in the country.

D. National computer emergency response team (CERT)/computer security incident response team (CSIRT)
CERT Vanuatu (CERT VU) was established to monitor, manage and mitigate cyber threats and vulnerabilities, either in selected organisations or throughout the entire country.

E. National cybersecurity strategy
The Vanuatu National Cyber Security Strategy (NCSS) 2023 was recently launched to strengthen national security and address cyber threats in Vanuatu. The strategy provides the government's plan on various national cybersecurity goals, objectives and priorities, and the level of cyber readiness and resilience to be achieved within the next ten years.

F. Initiatives to combat cybercrime
- Vanuatu was invited to accede to the Convention on Cybercrime (ETS No. 185) in 2021.
- Vanuatu is one of the 195 INTERPOL [881] member countries.[882]
- The facilitation of cybersecurity awareness courses both online and offline. For instance, sensitisation reminders are texted to people through their mobile network providers.[883]
- International co-operation and collaboration on cyber threats. The country's Cybercrime Act was passed, 'following the technical assistance received in 2018 from the Council of Europe[884] via its Global Action on Cybercrime Extended (GLACY+)[885] project'.[886] Since 2011, Vanuatu has been an active participant in the council's regional, international and national capacity building activities.[887]

56. Zambia

A. National cyber threat landscape
According to the National Cyber Security Index (NCSI),[888] as of January 2023 Zambia ranked 58th out of 161 countries on the NCSI with a score of 55.84; 73rd out of 194 countries on the Global Cybersecurity Index; 146th on the ICT Development Index; and 112nd on the Networked Readiness Index.

879 The Cybercrime Act, available at: https://ogcio.gov.vu/index.php/en/policy-legislation/legislation
880 Electronic Transactions Act, available at: http://www.paclii.org/vu/legis/consol_act/eta256/ (accessed 19 January 2023).
881 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
882 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).
883 'Cybersecurity and Safeguarding Electronic Transactions in the Pacific Islands', Policy Brief, available at: https://theprif.org/sites/default/files/documents/policy_brief_cyber_security_low_res_rev4.pdf (accessed 23 January 2023).
884 Council of Europe Office in Ukraine, 'About the Council of Europe', available at: www.coe.int/en/web/kyiv/the-coe/about-coe (accessed 31 January 2023).
885 Council of Europe, 'Global Action on Cybercrime Extended (GLACY)+, available at: www.coe.int/en/web/cybercrime/glacyplus (accessed 31 January 2023).
886 'Cybersecurity and Safeguarding Electronic Transactions in the Pacific Islands', Policy Brief, available at: https://theprif.org/sites/default/files/documents/policy_brief_cyber_security_low_res_rev4.pdf (accessed 23 January 2023).
887 Council of Europe, 'Vanuatu Engaged in Work on Data Protection Legislation', available at: www.coe.int/en/web/data-protection/-/vanuatu-engaged-in-work-on-data-protection-legislation (accessed 31 January 2023).
888 NCSI: Zambia, available at: https://ncsi.ega.ee/country/zm/ (accessed 14 January 2023).

B. National cybercrime legislation and related laws
- Cyber Security and Cyber Crimes Act 2021[889]
- Electronic Communications and Transactions Act 2021 (ECTA),[890] which repealed the Electronic Communications and Transactions Act 2009
- Information and Communications Technologies Act 2009

C. Scope/application of laws
- The Cyber Security and Cyber Crimes Act 2021 is the major substantive law that provides for cybercrime in Zambia. Part VI of the Act provides for the interception of communications, while Part IX provides specifically for cybercrimes in sections 49 to 71.
- The Electronic Communications and Transactions Act 2021 repealed and replaced the ECTA 2009. It aims to provide a safe and effective environment for electronic transactions.
- The Information and Communications Technologies Act 2009 repeals the Telecommunications Act and Radio Communications Acts of 1994. It provides the framework for ICT law and protection of the interests of service providers and consumers in Zambia.

D. National computer emergency response team (CERT)/computer security incident response team (CSIRT)
Zambia Computer Incident Response Team[891] co-ordinates cyber responses and manages cybersecurity incidents in Zambia.

E. National cybersecurity strategy
Zambia's National Cybersecurity Policy 2021[892] establishes a co-ordinated cybersecurity framework, with the aim to enhance the resilience of national ICT systems to cyber incidents and create a digitalised Zambia that is underpinned by trust and confidentiality. The policy also aims at reforming the legal and regulatory framework on cybersecurity and cybercrimes in the country.[893]

F. Initiatives to combat cybercrime
- Zambia is one of the 195 INTERPOL [894] member countries.[895]
- Establishment of a CIRT[896] to co-ordinate cyber responses and manage cybersecurity incidents in Zambia.
- Establishment of organisations such as the National Cyber Security Technical Committee (NCSTC) and the National Cyber Security, Advisory and Coordinating Council, which oversee incidents of cyber threats in the country.
- Presence of a Central Monitoring and Co-ordination Centre to ensure a co-ordinated attempt to analyse and monitor cyber incidents in the country.

889 Cyber Security and Cyber Crimes Act 2021, available at: www.parliament.gov.zm/sites/default/files/documents/acts/Act%20No.%202%20of%202021The%20Cyber%20Security%20and%20Cyber%20Crimes.pdf (accessed 15 January 2023).
890 National Assembly of Zambia, The Electronic Communications and Transactions Act 2021, available at: www.parliament.gov.zm/node/8842 (accessed 15 January 2023).
891 Zambia Computer Incident Response Team, available at: http://www.cirt.zm/ (accessed 13 January 2023).
892 National Cybersecurity Policy 2021, available at: www.zicta.zm/storage/sites/attachments/TVV4W9VO7MgqBMtdHT4h09NNq8XSXyS3VVYU44PF.pdf (accessed 23 January 2023).
893 Ibid.
894 The International Criminal Police Organization, available at: www.interpol.int/en (accessed 26 January 2023).
895 INTERPOL member countries, available at: www.interpol.int/en/Who-we-are/Member-countries (accessed 31 January 2023).
896 Zambia Computer Incident Response Team, available at: http://www.cirt.zm/ (accessed 13 January 2023).

- Formulation of a National Cybersecurity Policy,[897] the aim which is to: 'establish a coordinated cybersecurity framework and enhance resilience of national ICT systems to cyber incidents in order to attain the desired transformation into a Smart Zambia that is underpinned by trust and confidentiality. The Policy also aims at reforming the legal and regulatory framework on cybersecurity and cybercrimes in the country'.[898]
- Zambia co-operates and collaborates regionally and internationally with institutions and other countries to combat cybercrime, with supervisory authority resting with the Zambia Information and Communications Technology Authority.
- Zambia has ratified the African Union Convention on Cyber Security and Personal Data Protection ('the Malabo Convention') 2014.

897 National Cybersecurity Policy 2021, available at: www.zicta.zm/storage/sites/attachments/TVV4W9VO7MgqBMtdHT4h09NNq8XSXyS3VVYU44PF.pdf (accessed 23 January 2023).
898 Ibid.

Conclusions

This report shows that many Commonwealth countries have adopted legislation to address the problem of cybercrime. However, many legislative, policy, institutional and capacity gaps remain. In many cases, legislation adopted in the early 2000s is in need of revision and strengthening to address new and emerging cybercrime and cybersecurity threats.

Cybercrime and cybersecurity challenges threaten the economic, social, political and national security interests of countries. And with the increase in malware-for-hire services, increased sophistication of the criminals, and the emergence of generative artificial intelligence systems some of which can be used to generate tools and communications that can be used to commit acts of cybercrime it is imperative that Commonwealth countries strengthen their capacity to prevent, respond, investigate and prosecute cyber-crime and bring those responsible to justice irrespective of where they may be located.

Although limited in scope, this research shows that much has been done to address cybercrime, but a lot more needs to be done to ensure that all Commonwealth member countries have effective laws, poli-cies, institutions and multilateral cooperation frameworks to withstand the tide that is cybercrime. In the end, much will be achieved through closer collaboration and a recommitment to and an updating of the Commonwealth Cyber Declaration that was adopted by Commonwealth Heads of Government in 2018.

Many of Commonwealth Small States lack resources and capacity to unilaterally strengthen their anti-cyber-crime frameworks and to influence ongoing global efforts to influence the development of legal, policy and practice principles, including as enumerated in the proposed UN treaty on cybercrime. This raises the need for greater investment in cyber diplomacy and policy-influencing initiatives to protect the economic, social, political and security interests of Commonwealth member countries through addressing the interlinked challenges posed by the ever-expanding cybercrime and cybersecurity threats.

Equally, capacity building training and related technical assistance programmes directed especially at Commonwealth Small are required, including support that will enable them to engage in cyber diplomacy more effectively. In all, the imperative has grown to build an effective and sustainable Commonwealth anti-cyber cooperation framework.

Annex

The Commonwealth and Cybercrime Initiatives

The Commonwealth Secretariat ('the Secretariat') has undertaken cyber capacity development as a key strategy to enhance cyber governance and cyber resilience in Commonwealth member countries. Cybersecurity has been central to such efforts, including promoting the rule of law and responsible state behaviour in cyberspace, enhancing appropriate cybersecurity/cybercrime law making, promoting cybercrime policing in line with global best practices, and ensuring the protection of human rights and fundamental freedoms while employing measures to prevent and combat cybercrime.

Since the adoption of the Model Law on Computer and Computer Related Crime and the Commonwealth Cyber Declaration, with the financial support of the United Kingdom's Foreign and Commonwealth Office (UK FCDO), the Commonwealth Secretariat has continued to work on projects to implement the commitments of the Cyber Declaration across the Commonwealth. In this regard, the Secretariat works with national, regional and international partners to provide clear, detailed and sustainable help to member states to build capabilities to combat cybercrime by carrying out several projects aimed at strengthening the cyber resilience of member countries.

1. **Cybercrime awareness and capacity building**: in collaboration with several partners, the Secretariat held four regional conferences (Africa, Caribbean, Asia and Pacific) between January 2022 to February 2023 to raise awareness and enhance anti-cybercrime and cybersecurity capacity in Commonwealth member states. [899] The aim of the conferences was to increase awareness, influence cybercrime policies in Commonwealth member countries, and build capacity for law enforcement officials, prosecutors, judges and magistrates on cybercrime matters. The conferences also provided a platform for participants to exchange views on best practices and approaches to investigation, prosecuting and adjudicating over cybercrime cases and to develop a regional network of cybercrime experts necessary to promote enhanced collaboration for addressing cybercrime.[900]

2. **Cybersecurity needs assessment projects**: the Secretariat has also undertaken a cybersecurity/cybercrime needs assessment in some target countries. The objective of this project was to investigate the legislative and criminal justice response capabilities of each of the countries. The research undertook comprehensive reviews of the cyber resilience capabilities in each of the countries and recommended appropriate legislative responses in line with international best practice, the Commonwealth Model Law on Computer and Computer Related Crimes, as well as the Budapest Convention. In this way, key areas that required updating to provide an effective response to cyber threats were identified to improve cyber resilience in the countries.

3. **Technical assistance:** the Secretariat continues to render **t**echnical assistance to member countries through projects such as **t**he Commonwealth Network of Contact Persons Project (CNCP Project), which aims to enhance pan-Commonwealth and international co-operation in cross-border cybercrime investigations, leading to faster and more efficient prosecutions and greater integrity of electronic evidence in cross-border trials. In 2019, the Commonwealth Secretariat held three regional workshops on enhancing co-operation and strengthening capacity in obtaining digital evidence in

899 International Criminal Police Organization (Interpol), National Crime Agency (UK), META, Microsoft, UK Home Office, UN Women, United Nations Office on Drugs and Crime (UNODC), Council of Europe, The Caribbean Community (CARICOM) Implementation Agency for Crime and Security (IMPACS), Attorney General Alliance (AGA), Global Forum on Cyber Expertise (GFCE).

900 For the African Conference, which was held in Ghana, delegates were drawn from Nigeria, Ghana, Mauritius, Seychelles, Kenya, Namibia, Cameroon, Lesotho, Malawi, The Gambia and Sierra Leone; for the Caribbean Conference, held in Barbados, delegates were drawn from Barbados, Jamaica, Belize, Saint Lucia, St Vincent and the Grenadines, The Bahamas, Dominica, Guyana, Grenada, Antigua, and St Kitts and Nevis; the Asia conference was held in Singapore and delegates were drawn from Bangladesh, Brunei, Maldives, Malaysia, Singapore and Sri Lanka; and delegates for the Pacific conference, which were mainly judicial officials, were from PNG, Kiribati, Samoa, Solomon Islands, Nauru and Fiji.

cross-border cybercrime and terrorism investigations. This led to greater understanding of electronic evidence, fluent co-operation in trans-border cybercrime investigations and a greater understanding of new developments in legal mechanisms for obtaining electronic evidence from abroad.

4. **Cyber Declaration Programme**: The Commonwealth Secretariat has also focused on building capacity for cybersecurity legislation through the implementation of the Cyber Declaration. The Commonwealth Secretariat has worked on four distinct projects in order to implement the commitments of the Cyber Declaration across the Commonwealth, including the Africa Cyber Resilience Project, Electronic Evidence Training in the Caribbean, the International Co-operation Project and the Election Cybersecurity Project.

5. **The Commonwealth Cyber Fellowship (CACF):** The Commonwealth Cyber Fellowship was launched in July 2022. The aim of the CACF is to support member countries strengthen their cybersecurity and cybercrime frameworks by creating a trusted network of experts to enhance regional cyber capability and provide a platform for experts to share expertise and best practice in Africa.

6. **The Commonwealth 18–20 Fund:** The Commonwealth 18–20 Fund has helped more than 40 Commonwealth nations, especially smaller Commonwealth countries, to develop their national computer emergency response team (CERT/CSIRT) and has provided support for establishing dedicated teams that will respond swiftly to cyber threats and attacks.

7. **Certified cybersecurity training in the Caribbean**: the Secretariat, in collaboration with the Regional Security System (RSS), delivered a certified cybersecurity training for members of the Caribbean police force in Barbados in March 2023. The objective of the training was to create a pool of certified cybersecurity experts in the Caribbean police force.

8. **Cybersecurity knowledge products:** The Commonwealth Secretariat has developed various knowledge products to support cybersecurity capacity building in Commonwealth member states. These knowledge products/toolkits include:[901]
   - *the Commonwealth Election Cybersecurity Manual;*
   - the Commonwealth E-course on Electronic Evidence platform;
   - the Wiki- Commonwealth Cybercrime and Cybersecurity repository Microsoft Power BI;
   - *the Commonwealth Cybercrime Journal*: Volume 1, issue 1 | Commonwealth (thecommonwealth.org);
   - *the Commonwealth Cybercrime Monitor*[902] (a casebook on cybercrime in Commonwealth member states); and
   - research reports on emerging and contemporary issues on cybercrime in Commonwealth member countries.

901 Available at: www.thecommonwealth-ilibrary.org/index.php/comsec/catalog/category/Cybercrime
902 Available at: www.thecommonwealth-ilibrary.org/index.php/comsec/catalog/book/1101

Commonwealth Secretariat
Marlborough House, Pall Mall
London SW1Y 5HX
United Kingdom

thecommonwealth.org

The Commonwealth

D16191