CYBER SECURITY LAWS FOR OIC MEMBERS

September 2023

Prepared by:

Contents

1. INTRODUCTION

The Organization of Islamic Cooperation (OIC) Computer Emergency Response Team (CERT) is a network of national CERTs from member countries that aims to improve cybersecurity in the Islamic world. Cybercrime is a significant challenge in the digital age, and OIC-CERT member countries have responded by enacting various cyberlaws and regulations to combat cyber threats.

Many OIC-CERT member countries have enacted comprehensive cyberlaws and regulations to address cybercrime. These laws are designed to address various aspects of cybersecurity, including data protection, cybercrime prevention, and incident response. Here's a general introduction to the key areas of cybersecurity laws that OIC member states may have:

1. **Data Protection and Privacy Laws:** Many OIC member states have data protection and privacy laws that govern the collection, storage, and use of personal and sensitive data. These laws often align with international standards, such as the General Data Protection Regulation (GDPR), to protect individuals' privacy rights.
2. **Cybercrime Laws:** OIC member states typically have laws that criminalize various cybercrimes, such as hacking, identity theft, fraud, and the spread of malware. These laws establish penalties for individuals or organizations engaged in illegal online activities.
3. **Electronic Transactions and E-Signatures:** Some OIC member states have laws that recognize electronic transactions and electronic signatures as legally binding. These laws facilitate e-commerce and secure online transactions.
4. **Critical Infrastructure Protection:** Certain member states have laws and regulations aimed at protecting critical infrastructure sectors, such as energy, telecommunications, and finance, from cyber threats and attacks.
5. **Incident Reporting and Response:** OIC member states may have regulations requiring organizations to report cybersecurity incidents to relevant authorities or cybersecurity agencies. They may also establish frameworks for responding to and mitigating cyber incidents.
6. **National Cybersecurity Strategies:** Several OIC member states have developed national cybersecurity strategies that outline their approach to cybersecurity, including policy objectives, risk assessment, and capacity-building efforts.

Moreover, cybercrime is a constantly evolving threat, and new forms of cyber-attacks and crimes emerge all the time. Therefore, OIC-CERT member countries must work together to share information, best practices, and resources to combat cyber threats effectively. This includes promoting international cooperation and collaboration to combat cross-border cybercrime.

2. AIMS AND OBJECTIVES

This document aims to serve as a valuable resource for legal professionals, cyber security experts, researchers, and organizations operating in the OIC-CERT member countries. By offering a comprehensive overview of cyber security laws, their implications, and their enforcement mechanisms, the document intends to enhance legal understanding, compliance, and cooperation in addressing cyber threats and cybercrime across the OIC-CERT member states.

The objectives are:

- To contribute to the enhancement of regional cyber security efforts by providing valuable insights and legal clarity that can aid in addressing cyber threats and promoting a secure digital environment across OIC-CERT member states.
- To present real-world examples, case studies, and legal precedents that highlight the application and enforcement of cyber security laws, with a focus on the Computer Misuse Act, within OIC-CERT member countries.
- To clarify the roles and responsibilities of national Computer Emergency Response Teams (CERTs) and other relevant agencies in incident response and reporting procedures as governed by cyber security laws.

The purpose of this legal reference document is to compile and provide an in-depth analysis of cyber security-related laws and regulations, with a specific focus on the Computer Misuse Act or equivalent legislation, within the member countries of the Organization of Islamic Cooperation Computer Emergency Response Teams (OIC-CERT).

3. SCOPE

The scope of compiling cybersecurity laws is essential for legal professionals, policymakers, cybersecurity experts, and anyone involved in ensuring compliance with and enforcement of cybersecurity regulations.

- **Enhancing National Security**: Cybersecurity laws typically define and criminalize various cybercrimes, including unauthorized access, data breaches, and online fraud. They outline penalties for offenders and establish procedures for law enforcement agencies to investigate and prosecute cybercriminals.

- **Critical Infrastructure Protection:** These laws often focus on protecting critical infrastructure sectors, such as energy, telecommunications, and finance, from cyber threats. They may require organizations in these sectors to implement specific cybersecurity measures and reporting mechanisms for incidents.

- **Data Protection and Privacy:** Cybersecurity laws can include provisions related to data protection and privacy. They define how personal and sensitive data should be handled, stored, and protected, and they may establish rights for individuals regarding their personal information.

- **Incident Response and Reporting:** Laws often require organizations to report cybersecurity incidents to relevant authorities or cybersecurity agencies. They may also outline the procedures for incident response and recovery.

- **Regulation of Cybersecurity Service Providers:** Some laws may regulate cybersecurity service providers, such as managed security service providers (MSSPs), to ensure they meet specific standards and contribute to national cybersecurity efforts.

- **International Cooperation:** The scope can extend to provisions that promote international cooperation and information sharing on cyber threats and incidents among OIC member states.

4. OIC-CERT MEMBERS

4.1 AZERBAIJAN

Here are some of the key rules and regulations related to cybercrime in Azerbaijan:

1. **Law on Electronic Signature and Electronic Document (2004):** This law provides a legal framework for electronic transactions and establishes the requirements for electronic signatures and documents.
2. **Criminal Code of Azerbaijan (1999, amended in 2017):** This law includes provisions related to cybercrime, such as unauthorized access to computer systems, cyber espionage, and spreading malicious software.
3. **Law on Personal Data (2011):** This law sets out the rules for collecting, processing, and storing personal data in Azerbaijan.
4. **Law on Telecommunications (2005):** This law regulates the provision of telecommunications services in Azerbaijan, including the use of the internet.
5. **Law on Information, Informatization, and Protection of Information (2005):** This law sets out the rules for the protection of information, including electronic information, in Azerbaijan.
6. **National Strategy for Information Society Development (2017):** This strategy provides a framework for the development of Azerbaijan's information and communication technology (ICT) sector, including measures to enhance cybersecurity and combat cybercrime.
7. **Decree on the Establishment of the State Agency for Public Services and Social Innovations under the President of the Republic of Azerbaijan (ASAN Service) (2012):** This decree established ASAN Service, which is responsible for developing and implementing policies and strategies to combat cyber threats and promote cybersecurity in Azerbaijan.

These are some of the key rules and regulations related to cybercrime in Azerbaijan. The government of Azerbaijan has also established various other initiatives and measures to promote cybersecurity and combat cybercrime, such as the creation of the Electronic Security Service of the Ministry of Transport, Communications and High Technologies and the establishment of the National Computer Emergency Response Team (CERT).

The Criminal Code of Azerbaijan is the main legislation that sets out the criminal offenses and penalties related to cybercrime. The code was first adopted in 1999 and has been amended several times, most recently in 2017 to include provisions related to cybercrime.

The Criminal Code of Azerbaijan includes several provisions related to cybercrime, such as unauthorized access to computer systems, cyber espionage, and the spread of malicious software. The code also provides for criminal liability for offenses related to the theft or misappropriation of electronic data, as well as the creation, possession, or distribution of tools or software designed for the commission of cybercrimes.

Unauthorized access to computer systems is defined as intentional access to a computer system or network without authorization, with the intention of obtaining information or data that is not intended to be disclosed to the offender. This offense is punishable by imprisonment for a term of up to three years.

Cyber espionage is defined as the collection, analysis, or dissemination of confidential information through the use of computer systems or networks, without the permission of the relevant authorities. This offense is punishable by imprisonment for a term of up to eight years.

The spread of malicious software, such as viruses or malware, is also considered a criminal offense under the Criminal Code of Azerbaijan. This offense is punishable by imprisonment for a term of up to five years.

The code also includes provisions related to identity theft, cyber fraud, and other offenses related to computer and internet technology. For example, the code criminalizes the use of computer technology to defraud or deceive others, including through the use of false or misleading information.

Overall, the Criminal Code of Azerbaijan provides a legal framework for combating cybercrime and holds offenders accountable for their actions. The government of Azerbaijan has also established various initiatives and measures to promote cybersecurity and combat cybercrime, including the establishment of the National Computer Emergency Response Team (CERT) and the Electronic Security Service of the Ministry of Transport, Communications, and High Technologies.

4.2 BAHRAIN

The Computer Misuse Act in Bahrain was created in 2009. The act was enacted to address the growing threat of computer crimes, such as hacking and cyber-attacks, in the country and to provide a legal framework for dealing with these types of offenses. The act defines various computer-related crimes, including unauthorized access to computer systems, unauthorized modification of computer material, and unauthorized use of computer services. The act also provides for penalties for those convicted of computer crimes, including fines and imprisonment.

The specific year when the computer misuse and cybercrime act was created in Bahrain is not readily available. However, the Penal Code of Bahrain, which establishes criminal offenses related to cybercrime, was enacted in 1976. The Cybercrime Law of Bahrain, which specifically addresses cybercrime, was enacted at a later date, and the Electronic Transactions and Commerce Law, which provides the legal framework for electronic transactions and commerce in Bahrain, was enacted in 2002. The Regulation for the Protection of Personal Data, which provides for the protection of personal data in Bahrain, was enacted at a later date.

In Bahrain, the legal framework for combating cybercrime and addressing computer misuse is established by several laws and regulations, including the following:

1. **The Penal Code of Bahrain**: This law establishes criminal offenses related to cybercrime, such as hacking into computer systems, unauthorized access to computer systems, and the distribution of malicious software.
2. **The Cybercrime Law of Bahrain**: This law specifically addresses cybercrime and provides for the investigation, prosecution, and punishment of individuals who engage in illegal activities related to the use of information technology.
3. **The Electronic Transactions and Commerce Law of Bahrain**: This law provides the legal framework for electronic transactions and commerce in Bahrain and establishes rules for the protection of personal data and the security of electronic communications.
4. **The Regulation for the Protection of Personal Data**: This regulation provides for the protection of personal data in Bahrain and establishes the rights and obligations of individuals and organizations in relation to the processing of personal data.

In summary, the legal framework for combating cybercrime and addressing computer misuse in Bahrain is established by several laws and regulations, including the Penal Code, the Cybercrime Law, the Electronic Transactions and Commerce Law, and the Regulation for the Protection of Personal Data. These laws and regulations provide the framework for investigating, prosecuting, and penalizing individuals who engage in illegal activities related to the use of information technology, and for protecting the security of computer systems and networks and the privacy of personal data.

4.3 BANGLADESH

The Computer Misuse Act in Bangladesh was created in 2006. The act was enacted to address the growing threat of computer crimes, such as hacking and cyber-attacks, in the country and to provide a legal framework for dealing with these types of offenses. The act defines various computer-related crimes, including unauthorized access to computer systems, unauthorized modification of computer material, and unauthorized use of computer services. The act also provides for penalties for those convicted of computer crimes, including fines and imprisonment.

The Digital Security Act 2018 in Bangladesh contains several rules and regulations related to cybercrime. Here are some of the key provisions of the act:

1. **Unauthorized access:** It is illegal to gain unauthorized access to any computer, network, system, data, or information.
2. **Data theft:** It is illegal to intentionally or knowingly obtain or retain computer data or information without the owner's permission.
3. **Cyber stalking and bullying:** The act prohibits stalking, cyberbullying, and harassment of any person through digital means.
4. **Spreading fake news and propaganda:** It is illegal to spread false or fabricated information through digital media that may harm national security, public safety, or public order.
5. **Cyberterrorism:** The act criminalizes any act of terrorism committed using digital technology.
6. **Electronic transactions:** The act regulates electronic transactions and provides legal recognition for electronic signatures and electronic documents.
7. **Protection of critical information infrastructure**: The act provides for the protection of critical information infrastructure, including government networks and systems, banking and financial systems, and transportation and communication networks.
8. **Punishment**: The act outlines the punishments for various cybercrimes, including fines, imprisonment, or both.

It is worth noting that the Digital Security Act has been criticized by human rights organizations for potentially being used to suppress freedom of speech and curtail online dissent.

4.4 BRUNEI DARUSSALAM

The Computer Misuse Act (Chapter 194) is the primary legislation that provides for computer and cybercrime offences in Brunei Darussalam. The Act criminalizes offences including: unauthorised access to, and unauthorised modification of computer material; access with intent to commit or facilitate the commission of an offence; unauthorised use or interception of computer service; unauthorised obstruction of use of a computer; unauthorised disclosure of access codes; etc.

The Act also sets out the penalties for those found guilty of committing computer misuse offences. Penalties include fines, imprisonment, or both. The severity of the punishment depends on the nature and extent of the offense committed. There are also enhanced penalties for offences involving protected computers. The Act also provides for specific powers of investigation.

It is important to note that the Computer Misuse Act applies not only to computer systems and data, but also to other forms of digital technology, such as smartphones, tablets, and other internet-enabled devices.

In summary, the Computer Misuse Act in Brunei Darussalam is designed to protect the integrity and security of computer systems and data, as well as to deter those who may consider committing computer misuse offences. It is important for individuals and organizations in Brunei Darussalam to be aware of their obligations and responsibilities under this act, and to take appropriate measures to protect themselves from cybercrime.

The Computer Misuse Act in Brunei Darussalam outlines specific offences related to the misuse of computer systems and digital technology. The offences covered under the act include:

1. **Unauthorised access to computer material.**
2. **Access with intent to commit or facilitate commission of offence.**
3. **Unauthorised modification of computer material.**
4. **Unauthorised use or interception of computer service.**
5. **Unauthorised obstruction of use of computer.**
6. **Unauthorised disclosure of access code.**

In addition to the Computer Misuse Act, there are various other provisions under other laws that could also be used in the context of cybercrime and cyber-related offences in Brunei Darussalam. These laws include:

1. **Electronic Transactions Act (Chapter 196):** This Act provides a legal framework for electronic transactions, including electronic signatures and contracts, and establishes the validity and enforceability of electronic records.
2. **Penal Code (Chapter 22):** The Penal Code also criminalises certain offenses related to cybercrime, including identity theft, online harassment, online grooming, cyberstalking, etc.
3. **Telecommunications Order, 2001:** This order establishes the regulatory framework for telecommunications services, including internet services, and sets out the obligations of service providers to protect their customers' privacy and security; and
4. **Copyright Order, 1999**: This Order also provides for copyright infringements and protection, including those relating to telecommunications systems.
5. **Broadcasting Act, 1997**. An Act to regulate dealing in, the operation of and ownership in broadcasting services and broadcasting apparatus, and for connected purposes. This act was revised in the year 2000.

The **Cybersecurity Order, 2023** recently entered into force on 20 May 2023. It is an Order to require or authorize the taking of measures to prevent, manage and respond to cybersecurity threats and incidents, to regulate owners of critical information infrastructure and for matters related thereto.

It is important to note that Brunei's legal framework for cybercrime is still evolving, and the country continues to work on improving its cybersecurity infrastructure to protect against emerging threats in the digital age.

4.5 CÔTE D'IVOIRE

Côte d'Ivoire, also known as Ivory Coast, has laws and regulations that address computer-related offenses and cybercrime.

The country has a Cybersecurity Agency which is responsible for developing and implementing policies related to cybersecurity, and for coordinating the country's response to cyber threats. In addition, the government has enacted laws and regulations that aim to prevent cybercrime and protect the country's information systems.

One of the key laws related to cybercrime in Côte d'Ivoire is the Cybercrime Law, which was enacted in 2013. This law defines cybercrime and outlines the penalties for a range of offenses, including hacking, identity theft, and the distribution of malicious software. The law also includes provisions related to the protection of personal data, and establishes the National Cybersecurity Incident Response Team, which is responsible for responding to cyber threats.

In addition to the Cybercrime Law, Côte d'Ivoire has other laws that address cybercrime, including the Electronic Transactions Law and the Personal Data Protection Law. These laws set out rules for the use of electronic signatures and establish requirements for the protection of personal data.

Overall, Côte d'Ivoire has taken steps to address the threat of cybercrime, including the establishment of a dedicated cybersecurity agency and the enactment of laws and regulations aimed at preventing cybercrime and protecting the country's information systems.

The Cybercrime Law of Côte d'Ivoire, also known as Law No. 2013-450, is the main legislation that addresses cybercrime in the country. The law covers a wide range of offenses related to computer and Internet-based activities, including:

1. Unauthorized access to a computer system or network (hacking)
2. Interception of electronic communications
3. Distribution of malicious software (viruses, Trojans, etc.)
4. Identity theft and fraud
5. Online child pornography
6. Cyberstalking and harassment
7. Cyberterrorism
8. Unlawful use of electronic signatures
9. Unlawful interception or access to data

The law provides for severe penalties for those found guilty of committing cybercrimes, with fines and prison sentences ranging from one to ten years, depending on the offense.

In addition to the Cybercrime Law, Côte d'Ivoire has other laws and regulations that address specific aspects of cybersecurity, including the Electronic Transactions Law and the Personal Data Protection Law. These laws establish guidelines and requirements for the use of electronic signatures, protect personal data, and define the legal framework for e-commerce activities.

It is worth noting that these laws and regulations are constantly evolving as the threat landscape evolves, and Côte d'Ivoire, like many other countries, is continuously updating its legislation to address new and emerging cyber threats.

4.6 EGYPT

Egypt has several laws and regulations that address cybersecurity and the protection of personal data, including:

1. **The Egyptian Penal Code**: This law includes provisions that criminalize unauthorized access to computer systems and the theft of computer data.
2. **The Anti-Cyber and Information Technology Crimes Law**: This law was enacted to address the growing threat of computer crimes, such as hacking and cyber-attacks, in Egypt. The law defines various computer-related crimes and provides for penalties for those convicted of such crimes.
3. **The Personal Data Protection Law**: This law was enacted to protect the personal data of individuals in Egypt. The law requires organizations to obtain consent from individuals before collecting, processing, or using their personal data, and it also sets out requirements for the secure storage and transfer of personal data.
4. **The Electronic Signature Law**: This law provides the legal framework for the use of electronic signatures in Egypt, including requirements for the use of secure signature systems and the protection of signature data.

Egypt has implemented several measures to improve its cyber security and protect against potential threats. Some of the measures include:

1. **National Cybersecurity Strategy**: Egypt has a National Cybersecurity Strategy that outlines its approach to securing the country's digital infrastructure and critical information systems.
2. **Cybersecurity Law:** Egypt has a comprehensive Cybersecurity Law that defines cybercrime and outlines the measures that can be taken to prevent and prosecute cybercrime.
3. **Cybersecurity Centers:** Egypt has established several cybersecurity centers to monitor and respond to cyber threats in real-time. These centers are equipped with state-of-the-art technology and staffed by trained professionals.
4. **Public-Private Partnerships:** Egypt has also established partnerships with private sector companies to improve its cybersecurity posture. This collaboration allows for the sharing of information and resources between the public and private sectors.
5. **Awareness Campaigns:** Egypt has launched several awareness campaigns to educate the public about the importance of cybersecurity and how to protect against cyber threats.

These measures demonstrate Egypt's commitment to improving its cyber security and protecting against potential threats.

4.7 INDONESIA

Indonesia does not have a specific law that deals with computer misuse; however, the country has several laws and regulations that address various aspects of cybercrime. Some of the relevant laws and regulations include:

1. **Information and Electronic Transactions Law (ITE Law):** This law, enacted in 2008, provides the legal framework for e-commerce and electronic transactions in Indonesia. It also defines cybercrime and outlines penalties for various types of cybercrime, including hacking and online fraud.
2. **Criminal Code:** The Criminal Code of Indonesia contains provisions that address various forms of cybercrime, including computer-related fraud and hacking.
3. **Electronic System and Transaction Law:** This law, enacted in 2008, regulates the use of electronic systems and transactions in Indonesia, and includes provisions that address the use of digital signatures and secure electronic transactions.
4. **Decree of the Minister of Communications and Information Technology No. 16 of 2018:** This regulation outlines the procedures for reporting cyber incidents and the responsibilities of telecommunication service providers in preventing and addressing cybercrime.
5. **National Cyber and Encryption Agency (BSSN):** The BSSN is a government agency responsible for coordinating and implementing national cybersecurity policies and strategies. It also provides technical assistance and support to law enforcement agencies in investigating cybercrime.

These laws and regulations provide a framework for addressing computer misuse in Indonesia, but there is still room for improvement in terms of enforcement and the development of more specific regulations related to cybercrime.

Indonesia has a comprehensive national cybersecurity policy and strategy in place to protect its critical information infrastructure and digital assets. The following are some key elements of Indonesia's cyber security order:

1. **National Cyber and Encryption Agency (BSSN):** The BSSN is a government agency responsible for coordinating and implementing national cybersecurity policies and strategies. It also provides technical assistance and support to law enforcement agencies in investigating cybercrime.
2. **Information and Electronic Transactions Law (ITE Law):** This law, enacted in 2008, provides the legal framework for e-commerce and electronic transactions in Indonesia. It also defines

cybercrime and outlines penalties for various types of cybercrime, including hacking and online fraud.

3. **Criminal Code:** The Criminal Code of Indonesia contains provisions that address various forms of cybercrime, including computer-related fraud and hacking.
4. **Electronic System and Transaction Law:** This law, enacted in 2008, regulates the use of electronic systems and transactions in Indonesia, and includes provisions that address the use of digital signatures and secure electronic transactions.
5. **Decree of the Minister of Communications and Information Technology No. 16 of 2018:** This regulation outlines the procedures for reporting cyber incidents and the responsibilities of telecommunication service providers in preventing and addressing cybercrime.
6. **Cybersecurity Centers:** Indonesia has established several cybersecurity centers to monitor and respond to cyber threats in real-time. These centers are equipped with state-of-the-art technology and staffed by trained professionals.
7. **Public-Private Partnerships:** Indonesia has also established partnerships with private sector companies to improve its cybersecurity posture. This collaboration allows for the sharing of information and resources between the public and private sectors.
8. **Awareness Campaigns:** Indonesia has launched several awareness campaigns to educate the public about the importance of cybersecurity and how to protect against cyber threats.

These measures demonstrate Indonesia's commitment to improving its cyber security and protecting against potential threats. However, there is still room for improvement in terms of enforcement and the development of more specific regulations related to cybercrime.

It is important to note that Indonesia's legal framework for cybercrime is still evolving, and the country continues to work on improving its cybersecurity infrastructure to protect against emerging threats in the digital age.

4.8 IRAN

These laws and regulations provide a framework for addressing computer misuse in Iran, but there is still room for improvement in terms of enforcement and the development of more specific regulations related to cybercrime. Additionally, Iran's strict internet censorship and monitoring practices have led to concerns about privacy and freedom of speech.

Iran has several laws and regulations in place that address various aspects of cyber security, including the protection of critical information infrastructure and digital assets. The following are some key elements of Iran's cyber security order:

1. **Computer Crimes Law:** This law, enacted in 2009, defines computer crimes and outlines penalties for various types of cybercrime, including hacking, phishing, and spreading malicious software.
2. **Electronic Commerce Law:** This law, enacted in 2008, regulates electronic commerce in Iran and includes provisions that address the use of digital signatures and secure electronic transactions.
3. **Press Law:** The Press Law of Iran contains provisions that address the use of computer networks and the internet for the dissemination of information.
4. **Penal Code:** The Penal Code of Iran contains provisions that address various forms of cybercrime, including computer-related fraud and hacking.
5. **Cybercrime Investigation Office (CIO):** The CIO is a government agency responsible for investigating and prosecuting cybercrime in Iran.
6. **National Information Network (NIN):** The NIN is a national information and communication infrastructure that aims to provide secure and reliable communication services to government agencies and citizens.
7. **Cybersecurity Centers:** Iran has established several cybersecurity centers to monitor and respond to cyber threats in real-time. These centers are equipped with state-of-the-art technology and staffed by trained professionals.

These measures demonstrate Iran's commitment to improving its cyber security and protecting against potential threats. However, Iran's strict internet censorship and monitoring practices have led to concerns about privacy and freedom of speech. Additionally, there is still room for improvement in terms of enforcement and the development of more specific regulations related to cyber security.

4.9 JORDAN

Jordan has several laws and regulations related to computer misuse and cybersecurity. The primary legislation in this area is the Cybercrimes Law, also known as the Computer Misuse Act, which was enacted in Jordan in 2014. This law defines cybercrimes and outlines the penalties for such crimes, which can include imprisonment and/or fines.

Additionally, Jordan has also enacted the Cybersecurity Order, which is aimed at protecting critical information infrastructure and ensuring the country's cybersecurity. This order requires government agencies and private organizations to implement specific measures to protect against cyber threats and to report any incidents of cybercrime to the authorities.

The Cybersecurity Order also established the National Center for Security and Crisis Management, which is responsible for managing and responding to cyber security incidents in Jordan. The center also provides guidance and support to organizations on how to protect against cyber threats and to implement appropriate security measures.

Overall, Jordan has taken significant steps to address the issue of computer misuse and cyber security and has put in place a legal framework to help prevent and respond to cybercrimes.

Here is a list of some of the key cyber security orders and computer misuse acts in Jordan:

1. **The Cybercrimes Law, also known as the Computer Misuse Act**, enacted in 2014, which defines cybercrimes and outlines the penalties for such crimes.
2. **The Cybersecurity Order**, which requires government agencies and private organizations to implement specific measures to protect against cyber threats and to report any incidents of cybercrime to the authorities.
3. **The National Center for Security and Crisis Management**, established under the Cybersecurity Order, which is responsible for managing and responding to cyber security incidents in Jordan.
4. **The Electronic Transactions and Digital Signatures Law**, which governs the use of electronic transactions and digital signatures in Jordan and provides a legal framework for the protection of electronic communications and transactions.
5. **The Electronic Communications Law**, which governs the provision of electronic communications services in Jordan and sets out the obligations of service providers to protect the confidentiality and security of communications.

6. **The Personal Data Protection Law**, which governs the collection, use, and processing of personal data in Jordan and provides individuals with rights in relation to their personal data.

These laws and regulations form the legal framework for the protection of computer systems and information in Jordan and provide a framework for the investigation and prosecution of cybercrimes.

4.10 KAZAKHSTAN

Here is a list of some of the key cyber security orders and computer misuse acts in Kazakhstan:

1. The Law of the Republic of Kazakhstan "**On Information, Information Technologies and Information Protection**" - This law defines the legal framework for the use and protection of information, information technologies and personal data in Kazakhstan.
2. The Law of the Republic of Kazakhstan "**On Electronic Documents and Electronic Document Management**" - This law governs the use of electronic documents and establishes the legal basis for electronic document management in Kazakhstan.
3. The Law of the Republic of Kazakhstan "**On Personal Data and Protection of Privacy in Information and Communication Technologies**" - This law regulates the processing and protection of personal data in Kazakhstan and establishes the rights and obligations of data controllers and data processors.
4. The Decree of the President of the Republic of Kazakhstan "**On Approval of the National Plan for Information Security of the Republic of Kazakhstan for 2017-202**1" - This decree sets out the strategic goals and objectives for the protection of information and cybersecurity in Kazakhstan.
5. The Regulation of the Minister of Defense and Aerospace Industry of the Republic of Kazakhstan "**On the Procedure for Ensuring Information Security in the Defense and Aerospace Industry**" - This regulation establishes the procedures for ensuring information security in the defense and aerospace industry in Kazakhstan.
6. The Regulation of the Agency of the Republic of Kazakhstan for Communications and Information "**On Information Security Measures for the Provision of Communications Services**" - This regulation sets out the requirements for ensuring the security of communications services in Kazakhstan.

These laws and regulations form the legal framework for the protection of computer systems and information in Kazakhstan and provide a framework for the investigation and prosecution of cybercrimes.

4.11 KUWAIT

Here is a list of some of the key cyber security orders and computer misuse acts in Kuwait:

1. **The Electronic Transactions and Electronic Signatures Law** - This law governs the use of electronic transactions and digital signatures in Kuwait and provides a legal framework for the protection of electronic communications and transactions.
2. **The Personal Data Protection Law** - This law governs the collection, use, and processing of personal data in Kuwait and provides individuals with rights in relation to their personal data.
3. **The Law on Combating Cybercrimes** - This law defines cybercrimes and outlines the penalties for such crimes, which can include imprisonment and/or fines.
4. **The National Cybersecurity Strategy** - This strategy outlines the goals and objectives for protecting the country's critical information infrastructure and ensuring cybersecurity in Kuwait.
5. **The Regulation for the Protection of Information and Data in the Public Sector** - This regulation establishes the procedures for ensuring the security of information and data in the public sector in Kuwait.
6. **The Regulation for the Protection of Information and Data in the Private Sector** - This regulation establishes the procedures for ensuring the security of information and data in the private sector in Kuwait.

These laws and regulations form the legal framework for the protection of computer systems and information in Kuwait and provide a framework for the investigation and prosecution of cybercrimes.

4.12 KYRGYZSTAN

Kyrgyzstan has enacted several laws related to cyber security and the misuse of information technology. Here are a few of them:

1. Law on Information, Informatization, and Protection of Information (2005)
2. Law on Electronic Signature and Electronic Document (2008)
3. Law on Electronic Commerce (2010)
4. Law on Personal Data and Protection of Privacy (2012)
5. Law on Countering Terrorism and Extremism (2016)

It is important to note that the legal framework for cyber security and the protection of personal data in Kyrgyzstan is still evolving, and laws and regulations are subject to change.

However, the country has several laws and regulations that address unauthorized access to, and misuses of, computer systems and data.

Here are a few of the relevant laws:

1. Law on Information, Informatization, and Protection of Information (2005)
2. Criminal Code of Kyrgyz Republic (2004)
3. Law on Countering Terrorism and Extremism (2016)
4. Law on Electronic Signature and Electronic Document (2008)
5. Law on Personal Data and Protection of Privacy (2012)

It's worth noting that while these laws address various aspects of computer misuse, the legal framework in Kyrgyzstan is still evolving and may be subject to change.

4.13 LIBYA

Cybersecurity is an increasingly important issue in Libya and around the world, as more and more sensitive information is stored and transmitted online. To improve cybersecurity in Libya, the government could consider implementing a range of measures, such as:

1. Developing a national cybersecurity strategy that outlines the country's goals and priorities for protecting its critical information and infrastructure.
2. Improving cyber awareness and education programs to educate the public and businesses about the dangers of cybercrime and how to protect themselves and their data.
3. Building the capability of the country's law enforcement agencies to investigate and prosecute cybercrime.
4. Strengthening partnerships between the public and private sector to share information and best practices for preventing and responding to cyber incidents.
5. Providing incentives for companies to invest in cybersecurity, such as tax breaks, grants, or other forms of support.

It's important to note that cybersecurity is a complex and constantly evolving field, and no single measure can guarantee complete protection against cyber threats. However, by taking a comprehensive and proactive approach, governments can help to minimize the risks and improve the security of their critical information and infrastructure.

In Libya, cybercrime laws were in the process of development, but there may not have been comprehensive legislation in place at that time. Some of the common cybercrimes that were addressed under Libyan law, as of 2021, included:

1. **Unauthorized access to computer systems:** This typically involves illegal intrusion into computer systems, networks, or data without authorization.
2. **Data breaches and theft**: Unauthorized access to, acquisition, or dissemination of sensitive or confidential data is generally prohibited.
3. **Cyberbullying and harassment**: Harassing or bullying individuals online may be subject to legal action.
4. **Online fraud and scams**: Activities such as phishing, identity theft, and online fraud were likely covered under Libyan law.

5. **Distribution of malware and viruses**: Creating, distributing, or using malware and viruses with malicious intent may be considered a cybercrime.
6. **Intellectual property violations**: Unauthorized distribution or reproduction of copyrighted materials, software piracy, and other intellectual property violations may be addressed under the law.

4.14 MALAYSIA

Malaysia has been actively working to improve its cybersecurity posture in recent years. The Malaysian government has implemented several initiatives to enhance the country's cybersecurity, including the following:

1. **National Cybersecurity Strategy**: In 2016, the Malaysian government launched the National Cybersecurity Strategy, which outlines the country's goals and priorities for improving its cybersecurity posture. This strategy covers a range of areas, including cyber defense, critical information infrastructure protection, cybercrime investigation, and public education and awareness.
2. **Cybersecurity Regulatory Framework:** Malaysia has established a regulatory framework for cybersecurity, which includes laws and regulations designed to protect the country's critical information infrastructure, promote good cybersecurity practices, and criminalize cybercrime.
3. **Cybersecurity Incident Response Team**: The Malaysian Computer Emergency Response Team (MyCERT) was established to coordinate the country's response to cybersecurity incidents and to provide assistance to organizations and individuals affected by cyberattacks.
4. **Cybersecurity Awareness Campaigns:** The Malaysian government has launched several campaigns aimed at raising awareness about cybersecurity and encouraging individuals and organizations to adopt good cybersecurity practices.
5. **Cybersecurity Training and Education:** The Malaysian government has established programs to train and educate cybersecurity professionals and to promote cybersecurity awareness among the general public.

These initiatives demonstrate Malaysia's commitment to improving its cybersecurity posture and protecting its citizens and organizations from cyber threats. By taking a comprehensive and proactive approach to cybersecurity, Malaysia is working to minimize the risks and improve the security of its critical information and infrastructure.

The Computer Misuse Act (CMA) of Malaysia is a federal law that was enacted to address the growing threat of cybercrime in the country. The act provides for penalties for a range of computer-related offenses, including unauthorized access to computer systems, unauthorized modification of data, unauthorized use of computer systems, and the unauthorized distribution of malicious software.

Under the CMA, individuals who commit these types of offenses can be subject to fines and/or imprisonment, and companies can be held liable for the actions of their employees or agents. The act also provides for the forfeiture of any property or proceeds derived from the commission of a computer-related offense.

The CMA is designed to deter cybercrime and to provide a legal framework for investigating and prosecuting computer-related offenses. By criminalizing computer misuse and providing for penalties, the Malaysian government is working to protect the country's critical information infrastructure and to promote good cybersecurity practices.

4.15 MOROCCO

Morocco has enacted laws and regulations to address cybercrime and protect against online threats. The main laws related to cybercrime in Morocco include:

1. **The Moroccan Cybercrime Law:** This law criminalizes a range of cyber-related offenses, such as unauthorized access to computer systems, hacking, identity theft, and the spread of viruses or malware. The law also establishes penalties for these offenses and provides for cooperation with international law enforcement agencies.
2. **The Personal Data Protection Law**: This law regulates the collection, use, and disclosure of personal data, and establishes the rights of individuals to access, correct, and delete their personal information. It also requires organizations to take appropriate security measures to protect personal data.
3. **The Moroccan Telecommunications Act**: This act regulates the telecommunications sector, including internet services, and sets out the obligations of service providers to protect the privacy and security of their customers' data.
4. **The Moroccan Criminal Code**: This code criminalizes a range of offenses related to cybercrime, including fraud, forgery, and the distribution of obscene materials.
5. **The Moroccan Electronic Commerce Law**: This law establishes the legal framework for electronic commerce, including the rights and obligations of online service providers and consumers.

It is important to note that Morocco's legal framework for cybercrime is still evolving, and the country continues to work on improving its cybersecurity infrastructure to protect against emerging threats in the digital age.

4.16 NIGERIA

In Nigeria, the laws and regulations governing cybercrime include:

1. **Cybercrimes (Prohibition, Prevention, Etc.) Act 2015:** This is the primary law that criminalizes cybercrime in Nigeria. It provides for the prevention, detection, investigation, and prosecution of cybercrimes in the country. It also outlines the penalties for various types of cybercrimes, such as hacking, identity theft, cyber stalking, and cyber terrorism.
2. **Nigerian Communications Commission (NCC) Guidelines on SIM Card Registration:** This guideline mandates all network service providers to verify and register the personal details of all subscribers using a SIM card. This is aimed at reducing the incidence of SIM card fraud and other forms of cybercrime.
3. **Central Bank of Nigeria (CBN) Guidelines on Electronic Banking in Nigeria**: This guideline provides a regulatory framework for the operation of electronic banking in Nigeria. It outlines the responsibilities of financial institutions in ensuring the security of their electronic banking systems and protecting customers' confidential information.
4. **National Information Technology Development Agency (NITDA) Guidelines on Data Protection and Privacy: T**his guideline provides a framework for the protection of personal data and privacy in Nigeria. It mandates that individuals and organizations must obtain the consent of the data subject before collecting, processing, or sharing their personal data.
5. **Nigerian Cybercrime Advisory Council:** This is a council set up by the Nigerian government to provide advice on the prevention and detection of cybercrime. It also advises on the development of policies and strategies for combating cybercrime in the country.

Overall, these laws and regulations aim to protect individuals and organizations from the negative impact of cybercrime and ensure the responsible use of technology in Nigeria.

However, there is currently no law or regulation called the "Computer Misuse Act" in Nigeria. The Computer Misuse Act is a law in the United Kingdom that criminalizes various forms of cybercrime.

In Nigeria, the primary law that criminalizes cybercrime is the Cybercrimes (Prohibition, Prevention, Etc.) Act 2015. This Act criminalizes a wide range of offenses related to computer systems, networks, and other digital devices. Some of the key offenses under the Cybercrimes Act include:

1. Unauthorized access to computer systems or networks.
2. Hacking or attempting to hack computer systems or networks.
3. Intentionally spreading computer viruses or other malicious software.
4. Fraudulently obtaining data or personal information.
5. Identity theft and impersonation.
6. Cyberstalking and harassment.
7. Cyberterrorism.

The Cybercrimes Act also provides for the investigation, prosecution, and punishment of offenders. The penalties for cybercrime offenses vary depending on the specific offense committed and can range from fines to imprisonment. Overall, the Cybercrimes Act is aimed at combating cybercrime in Nigeria and ensuring the responsible use of technology in the country.

4.17 OMAN

In Oman, the law that criminalizes cybercrimes is the Cybercrime Law issued by Royal Decree 12/2011. This law outlines various cybercrimes and their penalties, and it aims to protect individuals and organizations from cyber threats.

Some of the key offenses under the Cybercrime Law in Oman include:

1. Unauthorized access to computer systems, networks, or data.
2. Hacking or attempting to hack computer systems or networks.
3. Disrupting computer systems, networks, or data.
4. Intentionally spreading computer viruses or other malicious software.
5. Fraudulently obtaining data or personal information.
6. Identity theft and impersonation.
7. Cyberstalking and harassment.

Using electronic means to facilitate the commission of other crimes, such as money laundering or terrorism.

The Cybercrime Law in Oman also provides for the investigation, prosecution, and punishment of offenders. The penalties for cybercrime offenses can range from fines to imprisonment, depending on the severity of the offense.

Overall, the Cybercrime Law in Oman is aimed at combating cybercrime in the country and protecting individuals and organizations from cyber threats. It is important to note that the law applies to both Omani nationals and foreign individuals who commit cybercrimes within the country's borders.

In Oman, the rules and regulations that govern cybercrime include:

1. **Cybercrime Law:** The Cybercrime Law issued by Royal Decree 12/2011 is the primary law that criminalizes cybercrime in Oman. This law criminalizes a wide range of cyber offenses, such as unauthorized access to computer systems, hacking, and spreading computer viruses or other malicious software.
2. **Telecommunications Regulatory Authority (TRA) Cybersecurity Framework:** The TRA is responsible for regulating and promoting the development of the telecommunications sector in Oman. It has developed a cybersecurity framework that outlines the guidelines for implementing

security measures to protect against cyber threats. The framework covers areas such as network security, data protection, and incident response.

3. **Data Protection Law**: The Data Protection Law regulates the collection, processing, and use of personal data in Oman. The law aims to protect the privacy of individuals and prevent the misuse of personal data by organizations. It also sets out the requirements for obtaining consent and the conditions for transferring personal data outside Oman.
4. **Oman Information Technology Authority (ITA) Cybersecurity Strategy**: The ITA is responsible for implementing the government's information technology policies and strategies. Its cybersecurity strategy outlines the government's approach to securing the country's information infrastructure against cyber threats. The strategy covers areas such as risk management, incident response, and cyber awareness.

Overall, these laws and regulations aim to combat cybercrime in Oman and ensure the responsible use of technology in the country. They provide a regulatory framework for the prevention, detection, investigation, and prosecution of cybercrime offenses and the protection of individuals and organizations from cyber threats.

4.18 PAKISTAN

Pakistan has two main laws that govern cybercrime and related offenses, which are the Prevention of Electronic Crimes Act 2016 and the Pakistan Electronic Crimes Act 2016. There is no law or regulation in Pakistan specifically called the "Computer Misuse Act."

The Prevention of Electronic Crimes Act (PECA) was passed in 2016, and it criminalizes a wide range of offenses related to electronic devices, networks, and digital data. Some of the key offenses under PECA include:

1. Unauthorized access to computer systems or data.
2. Hacking or attempting to hack computer systems or networks.
3. Disrupting or damaging computer systems or networks.
4. Intentionally spreading computer viruses or other malicious software.
5. Fraudulently obtaining data or personal information.
6. Identity theft and impersonation.
7. Cyberstalking and harassment.
8. Using electronic means to facilitate the commission of other crimes, such as terrorism or money laundering.

The Pakistan Electronic Crimes Act (PECA) was also passed in 2016, and it provides a legal framework for investigating and prosecuting cybercrime offenses. The Act outlines the procedure for obtaining search warrants, the rules of evidence for electronic data, and the jurisdiction of the courts for cybercrime cases.

The penalties for cybercrime offenses under these acts can vary depending on the severity of the offense and can include fines, imprisonment, and other penalties.

In addition to these laws, the Pakistan Telecommunication Authority (PTA) is responsible for regulating the telecommunications sector in Pakistan, and it has developed regulations related to cybercrime and cybersecurity. The PTA works with internet service providers and other organizations to monitor and block websites and online content that violates Pakistani laws or poses a threat to national security.

Overall, these acts aim to combat cybercrime in Pakistan and ensure the responsible use of technology in the country. They provide a legal framework for the prevention, detection, investigation, and prosecution of cybercrime offenses and the protection of individuals and organizations from cyber threats.

4.19 QATAR

In Qatar, cybercrime is governed by the Law on Combating Information Technology Crimes, which was enacted in 2014. The law aims to prevent and combat cybercrime by criminalizing a wide range of offenses related to the misuse of information technology.

Some of the key offenses under the law include:

1. Unauthorized access to computer systems or data.
2. Hacking or attempting to hack computer systems or networks.
3. Intentionally spreading computer viruses or other malicious software.
4. Identity theft and impersonation.
5. Cyberstalking and harassment.
6. Using electronic means to facilitate the commission of other crimes, such as terrorism or money laundering.

The law also provides for the investigation, prosecution, and punishment of offenders. The penalties for cybercrime offenses can range from fines to imprisonment, depending on the severity of the offense.

In addition to the Law on Combating Information Technology Crimes, the Ministry of Transport and Communications (MOTC) is responsible for regulating the telecommunications sector in Qatar, and it has developed regulations related to cybercrime and cybersecurity. The MOTC works with internet service providers and other organizations to monitor and block websites and online content that violates Qatari laws or poses a threat to national security.

Overall, the laws and regulations in Qatar aim to combat cybercrime and ensure the responsible use of technology in the country. They provide a legal framework for the prevention, detection, investigation, and prosecution of cybercrime offenses and the protection of individuals and organizations from cyber threats.

4.20 SAUDI ARABIA

In Saudi Arabia, cybercrime is governed by the Saudi Arabian Anti-Cybercrime Law, which was enacted in 2007 and has been amended several times. The law aims to combat cybercrime by criminalizing a wide range of offenses related to the misuse of information technology.

Some of the key offenses under the law include:

1. Unauthorized access to computer systems or data.
2. Hacking or attempting to hack computer systems or networks.
3. Disrupting or damaging computer systems or networks.
4. Intentionally spreading computer viruses or other malicious software.
5. Fraudulently obtaining data or personal information.
6. Identity theft and impersonation.
7. Cyberstalking and harassment.
8. Using electronic means to facilitate the commission of other crimes, such as terrorism or money laundering.

The law also provides for the investigation, prosecution, and punishment of offenders. The penalties for cybercrime offenses can range from fines to imprisonment, depending on the severity of the offense.

In addition to the Anti-Cybercrime Law, the National Cybersecurity Authority (NCA) was established in 2017 to regulate the country's cybersecurity and to protect critical infrastructure. The NCA works with government entities, critical infrastructure operators, and other organizations to assess their cybersecurity posture, identify vulnerabilities, and provide guidance on how to improve their cybersecurity defenses.

Overall, the laws and regulations in Saudi Arabia aim to combat cybercrime and ensure the responsible use of technology in the country. They provide a legal framework for the prevention, detection, investigation, and prosecution of cybercrime offenses and the protection of individuals and organizations from cyber threats.

The Saudi Arabian Cybersecurity Law was enacted in 2019 and became effective in January 2020. The law is intended to enhance the country's cybersecurity posture and protect critical infrastructure from cyber threats.

The Cybersecurity Law sets out a number of requirements for entities operating in Saudi Arabia, including:

1. Implementing appropriate cybersecurity measures to protect against cyber threats.
2. Conducting regular risk assessments and vulnerability testing.
3. Developing incident response plans and reporting any security incidents to the relevant authorities.
4. Appointing a dedicated cybersecurity officer to oversee cybersecurity efforts.
5. Protecting personal information and ensuring compliance with data protection laws.
6. Implementing measures to protect against cyber threats to critical infrastructure.

The Cybersecurity Law also establishes the National Cybersecurity Authority (NCA), which is responsible for regulating the country's cybersecurity and promoting cybersecurity awareness and best practices. The NCA works with government entities, critical infrastructure operators, and other organizations to assess their cybersecurity posture, identify vulnerabilities, and provide guidance on how to improve their cybersecurity defenses.

The Cybersecurity Law also outlines the penalties for non-compliance, which can range from fines to imprisonment, depending on the severity of the offense.

Overall, the Cybersecurity Law in Saudi Arabia demonstrates the country's commitment to enhancing its cybersecurity and protecting its critical infrastructure from cyber threats. The law sets out clear requirements for entities operating in the country and provides a legal framework for the prevention, detection, investigation, and prosecution of cybercrime offenses.

4.21 SOMALIA

Somalia did not have a comprehensive legal framework specifically addressing cybercrime. However, the country has criminal laws that may apply to cyber-related offenses, such as the Somali Penal Code, which prohibits unauthorized access to computer systems, fraud, and identity theft, among other offenses. The Penal Code also criminalizes the use of technology to facilitate terrorism and other serious crimes.

In addition, Somalia has taken steps to enhance its cybersecurity posture and combat cyber threats. For example, the Somali government has established the National Communications Authority (NCA), which is responsible for regulating the country's telecommunications and information technology sector. The NCA has issued regulations and guidelines to promote cybersecurity and protect against cyber threats, such as requiring service providers to implement appropriate technical and organizational measures to protect customer data and prevent cyber-attacks.

Somalia has also been working with international partners to enhance its cybersecurity capabilities and promote cybersecurity awareness. For example, the country is a member of the African Union's African Union Convention on Cyber Security and Personal Data Protection, which aims to promote cooperation among African countries to address cybercrime and protect personal data.

Overall, while Somalia may not have a comprehensive legal framework specifically addressing cybercrime, the country has taken steps to enhance its cybersecurity capabilities and combat cyber threats. The existing criminal laws may be used to prosecute cyber-related offenses, and the government has established regulations and guidelines to promote cybersecurity and protect against cyber threats.

4.22 SUDAN

Sudan did not have a specific law or comprehensive legal framework specifically addressing cybercrime. However, the country has several laws and regulations that may apply to cyber-related offenses, such as the Penal Code, the Electronic Transactions Act, and the Press and Publications Law.

The Sudanese Penal Code criminalizes a wide range of offenses that may apply to cybercrime, such as unauthorized access to computer systems, computer fraud, and identity theft. The Electronic Transactions Act provides a legal framework for electronic transactions and electronic signatures and may also apply to cyber-related offenses such as computer fraud and hacking. The Press and Publications Law may also apply to cyber-related offenses such as online defamation or hate speech.

Sudan had enacted the "Sudan Cybercrime Act of 2007" to address various aspects of cybercrime and electronic transactions.

Here are some key points related to the Sudan Cybercrime Act of 2007:

1. **Scope**: The law aimed to regulate various aspects of cybercrime, including unauthorized access to computer systems, data breaches, online fraud, and other electronic offenses.
2. **Penalties**: The act outlined penalties for various cybercrimes, which could include fines, imprisonment, or both, depending on the severity of the offense.
3. **Data Protection**: The law may have included provisions related to data protection and the security of personal information, although the level of detail and enforcement may vary.
4. **Electronic Transactions**: The act likely addressed legal aspects of electronic transactions, such as electronic contracts and electronic signatures, to promote e-commerce and digital business.
5. **Cybersecurity**: It might have included provisions related to the protection of critical information infrastructure and measures to enhance cybersecurity.
6. **Enforcement**: The act likely outlined the roles and responsibilities of law enforcement agencies and the judiciary in investigating and prosecuting cybercrimes.

In addition, Sudan has taken steps to enhance its cybersecurity capabilities and combat cyber threats. For example, the country has established the National Information Center (NIC), which is responsible for coordinating and implementing Sudan's cybersecurity strategy. The NIC has launched initiatives to raise awareness about cybersecurity risks and promote best practices to prevent cyber threats.

Sudan has also been working with international partners to enhance its cybersecurity capabilities and promote cybersecurity awareness. For example, the country is a member of the African Union's African

Union Convention on Cyber Security and Personal Data Protection, which aims to promote cooperation among African countries to address cybercrime and protect personal data.

Overall, while Sudan may not have a specific law or comprehensive legal framework specifically addressing cybercrime, the country has criminal laws that may apply to cyber-related offenses and has taken steps to enhance its cybersecurity capabilities and combat cyber threats.

4.23 SYRIAN ARAB REPUBLIC

Syria did not have a comprehensive legal framework specifically addressing cybercrime. However, the country has criminal laws that may apply to cyber-related offenses, such as the Syrian Penal Code, which prohibits unauthorized access to computer systems, fraud, and identity theft, among other offenses.

In addition, Syria has taken steps to enhance its cybersecurity posture and combat cyber threats. For example, the country has established the Syrian Computer Society, which is responsible for promoting the use of information technology and protecting against cyber threats. The Syrian Computer Society has launched initiatives to raise awareness about cybersecurity risks and promote best practices to prevent cyber threats.

The Syrian Arab Republic had enacted a law known as the "Cybercrime Act" (قانون جرائم المعلوماتية) which was promulgated in 2012. This law addresses various aspects of cyber-related offenses, including but not limited to:

1. Unauthorized access to computer systems or networks.
2. Interception or monitoring of data without authorization.
3. Distribution of malicious software (malware).
4. Online fraud and identity theft.
5. Cyberterrorism and cyberespionage.
6. Distribution of child pornography.
7. Violations related to electronic commerce and financial transactions.

Overall, while Syria may not have a comprehensive legal framework specifically addressing cybercrime, the country has criminal laws that may apply to cyber-related offenses and has taken steps to enhance its cybersecurity capabilities and combat cyber threats. However, due to ongoing conflicts and political instability, the implementation and enforcement of these laws may be limited.

4.24 TUNISIA

Tunisia has a comprehensive legal framework to combat cybercrime. The main law governing cybercrime in the country is the Law No. 2019-26 on Cybercrime, which was passed in 2019 and repealed the previous cybercrime law of 2004.

The Cybercrime Law defines and criminalizes a wide range of cyber-related offenses, including unauthorized access to computer systems, data interference, computer fraud, identity theft, and cyber espionage. The law also provides for the protection of critical infrastructure, the preservation of electronic evidence, and international cooperation in combating cybercrime.

In addition to the Cybercrime Law, Tunisia has other legal instruments that may apply to cybercrime, such as the Penal Code, the Electronic Commerce Law, and the Personal Data Protection Law.

Some key aspects of Tunisia's cybercrime laws and regulations as of 2021 included:

1. **Tunisian Cybercrime Law**: Tunisia enacted a specific cybercrime law, known as Law No. 2004-575 of July 22, 2004, which was amended in 2015. This law addresses various aspects of cybercrime, including unauthorized access to computer systems, data breaches, online fraud, and the dissemination of malicious software.
2. **Penalties**: The Tunisian Cybercrime Law prescribes penalties for different cybercrimes, including fines and imprisonment, depending on the severity of the offense.
3. **Data Protection**: Tunisia has also enacted data protection laws, which are designed to protect the privacy and personal information of individuals online. The Personal Data Protection Law (Law No. 63 of 2004) regulates the collection, processing, and transfer of personal data.
4. **Electronic Transactions**: Tunisia recognizes the legal validity of electronic contracts and signatures. This facilitates e-commerce and digital transactions.
5. **Cybersecurity**: The government of Tunisia has taken steps to enhance the country's cybersecurity infrastructure and protect critical information systems.
6. **National Computer Security Agency (ANSI)**: ANSI is responsible for coordinating efforts related to cybersecurity in Tunisia and implementing measures to counter cyber threats.
7. **International Cooperation**: Tunisia participates in international efforts to combat cybercrime and is a member of organizations like the African Union (AU) and the United Nations (UN) in addressing cybercrime issues.

4.25 TURKIYE

Turkiye has several laws and regulations that address computer-related offenses and cybercrime, including:

1. **Turkish Penal Code**: This code criminalizes various computer-related offenses, such as unauthorized access to computer systems, data theft, and use of personal data without consent. Offenders can face imprisonment and fines, depending on the severity of the offense and its consequences.
2. **Law No. 5651 on Regulation of Broadcasts via the Internet and Prevention of Crimes Committed Through Such Broadcasts**: This law criminalizes several cyber-related offenses, including spreading propaganda for a terrorist organization, access to personal data without authorization, and dissemination of sexual images of individuals without their consent.
3. **Law No. 6698 on the Protection of Personal Data**: This law regulates the protection of personal data and establishes obligations for data controllers and processors. It also includes provisions related to the handling of personal data in the context of cybersecurity incidents.
4. **Electronic Communications Law**: This law regulates electronic communications and includes provisions related to the confidentiality and security of communications, as well as the protection of personal data.
5. **Cyber Security Strategy and Action Plan**: This plan, adopted by the Turkish government in 2013, outlines Turkey's strategy for enhancing cybersecurity and combating cyber threats. It includes measures to improve the security of critical infrastructure, promote cybersecurity awareness, and develop a skilled cybersecurity workforce.

Overall, Turkiye has a legal framework that addresses computer-related offenses and cybercrime. However, like many countries, Turkiye faces challenges in effectively addressing the evolving nature of cyber threats and ensuring the security of its information systems.

4.26 UNITED ARAB EMIRATES

The United Arab Emirates (UAE) does not have a specific Computer Misuse Act, but its Federal Law No. 5 of 2012 on Combating Cyber Crimes addresses a range of computer-related offenses and cybercrime. This law criminalizes several cyber activities, including unauthorized access to computer systems, data theft, cyber espionage, identity theft, and hacking. The law also establishes penalties for these offenses, ranging from fines to imprisonment and deportation for foreign offenders. Additionally, the Telecommunications Regulatory Authority (TRA) has issued guidelines for the telecommunications sector to protect against cyber threats, including security measures to safeguard networks and data from cyber-attacks. Overall, the UAE's legal framework for cybercrime addresses a range of computer-related offenses and seeks to protect against cyber threats to ensure the security of critical infrastructure.

The United Arab Emirates (UAE) has several key cybersecurity orders in place, including:

1. **UAE Cybersecurity Law**: This law, which came into effect in 2019, outlines the responsibilities of government entities, private companies, and individuals with respect to cybersecurity. The law also establishes a national cybersecurity strategy and a framework for reporting and responding to cyber incidents.
2. **National Electronic Security Authority (NESA) Regulations**: The NESA is the UAE's federal authority for information security and cybersecurity. The NESA regulations set out standards for securing government systems and networks, as well as guidelines for other entities to implement cybersecurity best practices.
3. **Dubai Cybersecurity Law:** In 2020, the Dubai government passed a cybersecurity law that requires companies operating in the emirate to implement cybersecurity measures and report cyber incidents to the relevant authorities.
4. **Abu Dhabi Digital Authority (ADDA) Information Security Regulation:** The ADDA is responsible for overseeing the digital transformation of Abu Dhabi, including the security of digital systems and services. The ADDA's information security regulation includes guidelines for organizations to protect against cyber threats.
5. **Telecommunications Regulatory Authority (TRA) Cybersecurity Regulatory Framework:** The TRA is responsible for regulating the telecommunications sector in the UAE, including the security of telecommunications networks and services. The TRA's cybersecurity regulatory framework includes guidelines for telecommunications providers to protect against cyber threats.

These cybersecurity orders and regulations are designed to protect against cyber threats and promote the security of critical infrastructure in the UAE.

4.27 UGANDA

The Computer Misuse Act, 2011 is the primary legislation in Uganda that deals with computer-related crimes and cybersecurity. Here's a more detailed overview of some of the key provisions and aspects of this act:

1. **Unauthorized Access (Section 4):**

   The act prohibits unauthorized access to computer systems. This includes accessing computer systems, programs, or data without permission.

2. **Unauthorized Modification of Content (Section 5):**

   It is illegal to make unauthorized modifications to computer data, programs, or systems. This provision is aimed at preventing activities such as hacking and data tampering.

3. **Unauthorized Interception of Communications (Section 6):**

   Intercepting or monitoring communications (e.g., emails, messages) without proper authorization is prohibited.

4. **Unauthorized Disclosure of Passwords and Access Codes (Section 7):**

   The act prohibits the unauthorized disclosure of passwords, access codes, or any other means of accessing computer systems or data.

5. **Making, Supplying, or Obtaining Anything for Use in Offenses (Section 8):**

   It's an offense to create, supply, or obtain tools, software, or devices that are intended for use in computer-related crimes.

6. **Unauthorized Use or Possession of Computer Systems (Section 9):**

   This section addresses unauthorized use or possession of computer systems or data.

7. **Cyber Espionage (Section 10):**

   The act also covers cyber espionage, making it illegal to engage in activities that compromise national security through the misuse of computer systems.

8. **Penalties (Section 11):**

   The penalties for violations of the Computer Misuse Act can include fines and imprisonment. The severity of the penalty depends on the nature and gravity of the offense.

4.28 UZBEKISTAN

Uzbekistan has several laws and regulations that address computer-related offenses and cybercrime, including:

1. **Criminal Code of Uzbekistan**: This code criminalizes several computer-related offenses, such as unauthorized access to computer systems, data theft, and use of personal data without consent. Offenders can face imprisonment and fines, depending on the severity of the offense and its consequences.
2. **Law on Combating Cyber Attacks**: This law addresses various cyber threats and offenses, including illegal access to computer systems, theft of electronic information, and use of computer systems for fraud or extortion. The law also establishes the Computer Emergency Response Team (CERT) as the central authority responsible for coordinating and responding to cyber incidents in Uzbekistan.
3. **Law on Personal Data:** This law regulates the collection, processing, and storage of personal data in Uzbekistan. It includes provisions related to the security of personal data, as well as the rights of individuals to access and control their personal data.
4. **Law on Telecommunications:** This law regulates telecommunications activities in Uzbekistan, including the use of communication networks for illegal purposes. It includes provisions related to the confidentiality and security of communications, as well as the interception and monitoring of electronic communications for law enforcement purposes.
5. **National Program for Information Security:** This program was established in 2018 and outlines Uzbekistan's strategy for enhancing cybersecurity and combating cyber threats. It includes measures to improve the security of critical infrastructure, promote cybersecurity awareness, and develop a skilled cybersecurity workforce.

Overall, Uzbekistan has a legal framework that addresses computer-related offenses and cybercrime. However, like many countries, Uzbekistan faces challenges in effectively addressing the evolving nature of cyber threats and ensuring the security of its information systems.

The penalties for cybercrime offenses in Uzbekistan are outlined in the Law of the Republic of Uzbekistan "On Information, Informatization and Protection of Information". The exact penalties will depend on the specific nature and severity of the offense committed.

It is important to note that the penalties for cybercrime offenses in Uzbekistan are designed to deter individuals from engaging in illegal activities related to the use of information technology and to protect the integrity and security of computer systems and networks.

In conclusion, the penalties for cybercrime offenses in Uzbekistan can include fines and imprisonment, and the exact penalties will depend on the specific nature and severity of the offense committed.

5. CONCLUSION

In conclusion, OIC-CERT member countries have made significant progress in addressing cybercrime through the enactment of comprehensive cyberlaws and regulations. However, more needs to be done to improve cybersecurity across the Islamic world, and international cooperation is essential to combat cyber threats effectively. By working together, OIC-CERT member countries can create a safer and more secure digital environment for their citizens and businesses.

Addressing cybercrime and advancing cybersecurity is an ongoing journey that demands unwavering commitment, collaboration, and adaptability. While significant strides have been made in enacting cybercrime laws, fostering public awareness, and enhancing law enforcement capabilities, we must recognize that the cyber threat landscape is dynamic and ever evolving. To maintain progress in addressing cybercrime, we must continue to strengthen our legal frameworks, educate individuals and organizations, bolster international cooperation, and invest in cybersecurity infrastructure and innovation.

The battle against cybercrime is a collective endeavor that transcends borders and sectors. By working together, we can create a safer digital environment for all, protect critical infrastructure, and ensure the resilience of our societies in the face of cyber threats. It is not just a matter of technological defenses but also a commitment to cybersecurity as a shared responsibility. In this interconnected world, our vigilance and collaboration are the keys to building a more secure and resilient digital future.

6. REFERENCES

- https://cyberlaws.net/cyber-law-repository/cyber-laws-different-countries/
- https://www.csb.gov.bn/cyber-security-order (Brunei Darussalam)
- https://www.agc.gov.bn/AGC%20Images/LAWS/Gazette_PDF/2010/EN/S013.pdf (Brunei Darussalam)
- https://www.agc.gov.bn/AGC%20Images/LOB/pdf/Chp.180.pdf (Brunei Darussalam)
- https://www.ilo.org/dyn/natlex/docs/ELECTRONIC/83695/92621/F1512682825/AZE83695%202.pdf (Azerbaijan)
- https://www.asianlaws.org/gcld/cyberlawdb/GCC/Law%20on%20Combating%20Cybercrime%20in%20the%20Kingdom%20of%20Bahrain.pdf (Bahrain)
- https://www.cirt.gov.bd/wp-content/uploads/2020/02/Digital-Security-Act-2020.pdf (Bangladesh)
- https://www.dataguidance.com/notes/ivory-coast-data-protection-overview (Ivory Coast)
- https://cybercrime-fr.org/wp-content/uploads/2020/04/Egyptian-cybercrime-law-.pdf (Egypt)
- http://www.flevin.com/id/lgso/translations/JICA%20Mirror/english/4846_UU_11_2008_e.html (Indonesia)
- https://www.article19.org/data/files/medialibrary/2921/12-01-30-FINAL-iran-WEB%5B4%5D.pdf (Iran)
- https://cyrilla.org/api/files/158919505942963pqxl58e5s.pdf (Jordan)
- https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw.data_protection/functions/handbook.pdf?country-1=KZ#:~:text=Kazakh%20law%20requires%20to%20carry,confirm%20the%20receipt%20of%20consent (Kazakhstan)
- https://kdipa.gov.kw/wp-content/uploads/2022/08/%D9%82%D8%A7%D9%86%D9%88%D9%86-%D8%A7%D9%84%D9%85%D8%B9%D8%A7%D9%85%D9%84%D8%A7%D8%AA-%D8%A7%D9%84%D8%A7%D9%84%D9%83%D8%AA%D8%B1%D9%88%D9%86%D9%8A%D8%A9-20-%D9%84%D8%B3%D9%86%D8%A9-2014-%D9%85%D8%AA%D8%B1%D8%AC%D9%85-%D8%A8%D8%A7%D9%84%D9%84%D8%BA%D8%A9-%D8%A7%D9%84%D8%A7%D9%86%D8%AC%D9%84%D9%8A%D8%B2%D9%8A%D8%A9.pdf (Kuwait)
- https://www.citra.gov.kw/sites/en/LegalReferences/Data_Privacy_Protection_Regulation.pdf (Kuwait)
- https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw.data_protection/functions/handbook.pdf?country-1=KG (Kyrgyzstan)
- https://www.nacsa.gov.my/legal.php#:~:text=The%20Computer%20Crimes%20Act%201997,unauthorised%20modification%20of%20computer%20contents. (Malaysia)
- https://www.dlapiperdataprotection.com/system/modules/za.co.heliosdesign.dla.lotw.data_protection/functions/handbook.pdf?country-1=MA (Morocco)
- http://www.nigerianlawguru.com/legislations/STATUTES/CYBERCRIME%20ACT%202015.pdf (Nigeria)

- https://www.qcert.org/sites/default/files/public/documents/om-ecrime-issuing_the_cyber_crime_law-eng-2011.pdf (Oman)
- https://www.ita.gov.om/ITAPortal/MediaCenter/Document_detail.aspx?NID=54 (Oman)
- https://na.gov.pk/uploads/documents/1470910659_707.pdf (Pakistan)
- https://www.cra.gov.qa/-/media/System/F/5/5/8/F55881326A3857EEA2FDC4ECD9E188E0/2014-Law-No-14-Cybercrime-Prevention-Law-unofficial-translation-EN.ashx (Qatar)
- https://laws.boe.gov.sa/Files/Download/?attId=5386bb81-a4a9-44d5-865d-ad3c00bd0dff (Saudi Arabia)
- https://nca.gov.so/cybersecurity/ (Somalia)
- https://ictpolicyafrica.org/es/document/oi11tiq4rq?page=2 (Sudan)
- https://scm.bz/en/legal-review-of-the-cybercrime-law-no-20-of-2022/ (Syrian Arab Republic)
- https://mbkaya.com/turkish-internet-law/ (Turkiye)
- https://u.ae/en/resources/laws (UAE)
- https://ucudir.ucu.ac.ug/items/e6c1b6b6-02b2-4285-aafd-fd852f34251c/full (Uganda)
- https://lex.uz/uz/docs/5960604 (Uzbekistan)