www.itrc.ac.ir

به نام خدا

وزارت ارتباطات و فناوری اطلاعات

پژوهشگاه ارتباطات و فناوری اطلاعات

(مرکز تحقیقات مخابرات ایران)

ITRC

Cyber Crime Legislation

Presented By: Tala Tafazzoli

Date: May 2018

Cyber Crime

- There are at present a large number of terms used to describe crime involving computers.
- Such terms include
  - computer-related crime,
  - computer crime,
  - internet crime,
  - e-crime,
  - high-tech crime,
  - online crime,
  - electronic crime,
  - computer misconduct and
  - cybercrime.

Definitions of Cybercrime

- The USA Department of Justice defines computer crime as
  - "any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation or prosecution".

Definitions of Cybercrime

- The UK Association of Chief Police Officers (ACPO) has defined e-crime as
  - the "use of networked computers, telephony or internet technology to commit or facilitate the commission of crime"

Definitions of Cybercrime

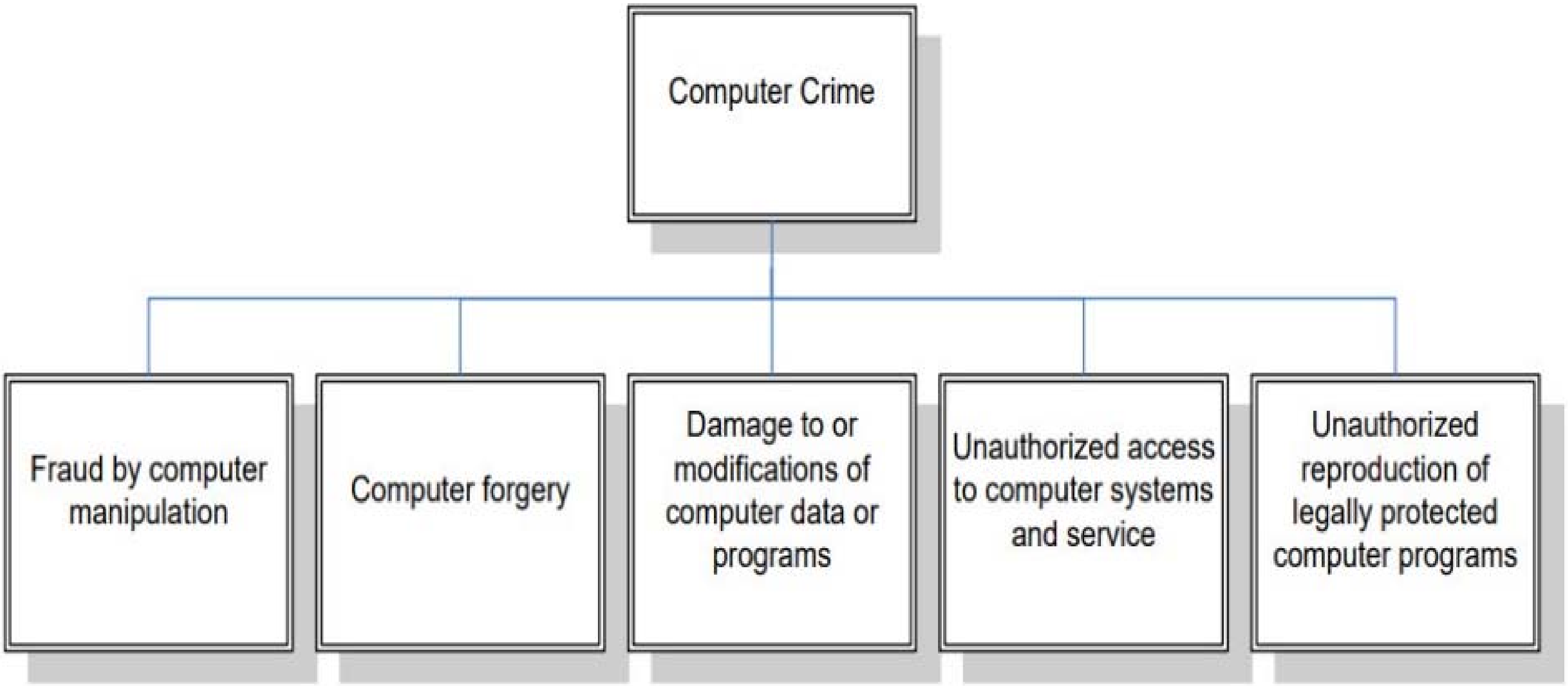
- Symantec Corporation defines cybercrime broadly as :
  - "any crime that is committed using a computer or network or hardware device".

Definitions of Cybercrime

- The Australian Centre for Police Research (ACPR) defines e-crimes (cybercrime) as:
  - "offences where a computer is used as a tool in the commission of an offence, as the target of an offence, or used as a storage device in the commission of an offence"

- computer crime or cybercrime is divided into three categories:
  - The use of computer as a target of criminal activity (e.g. hacking, dissemination of viruses)
  - The use of computer as a tool or instrument used to commit a criminal activity (e.g. online fraud)
  - The use of computer as incidental to the crime (e.g. data storage for criminal activity)

The common types of computer crime according to UN



Computer Crime

Fraud by computer manipulation

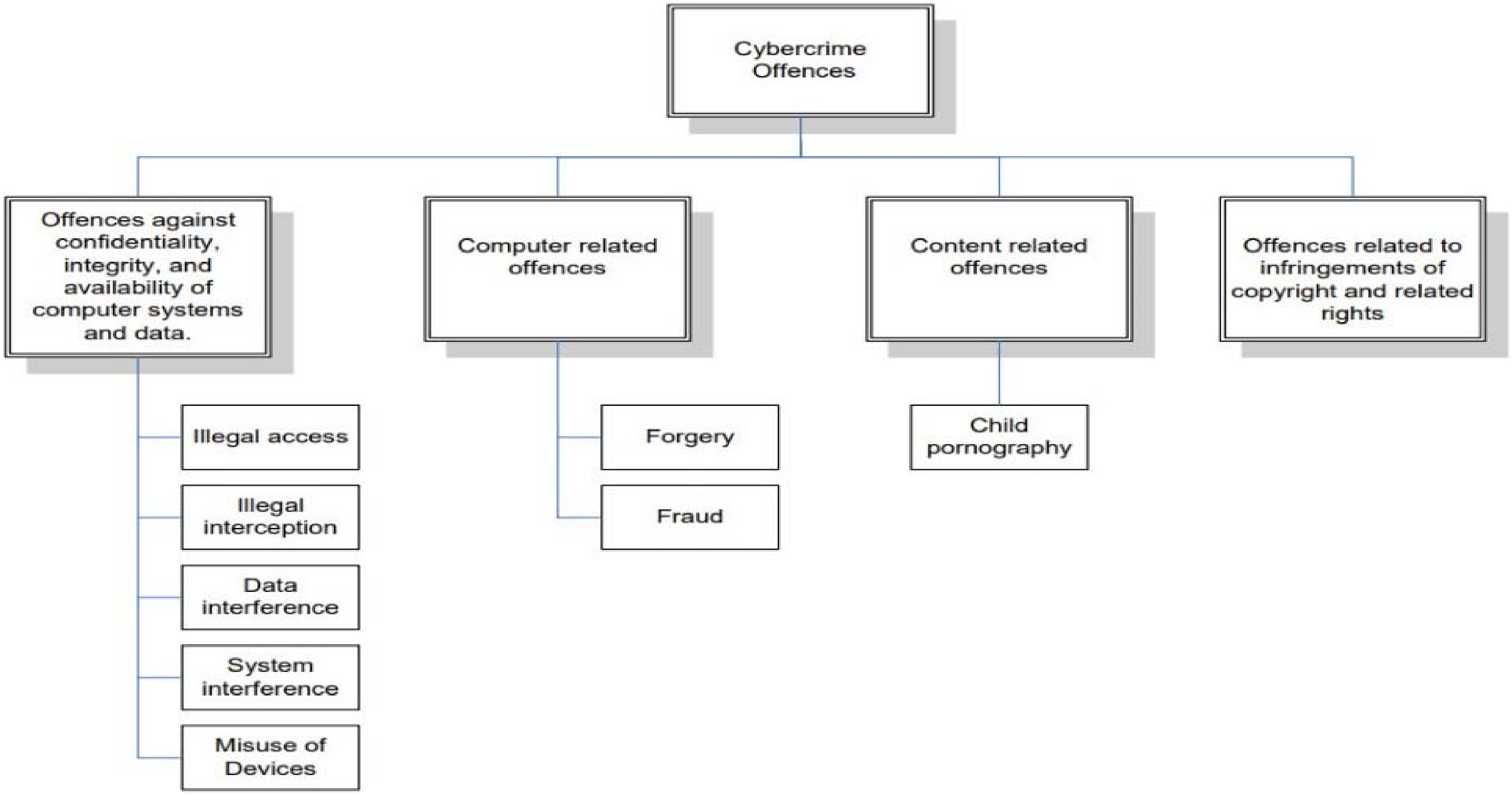
Computer forgery

Damage to or modifications of computer data or programs

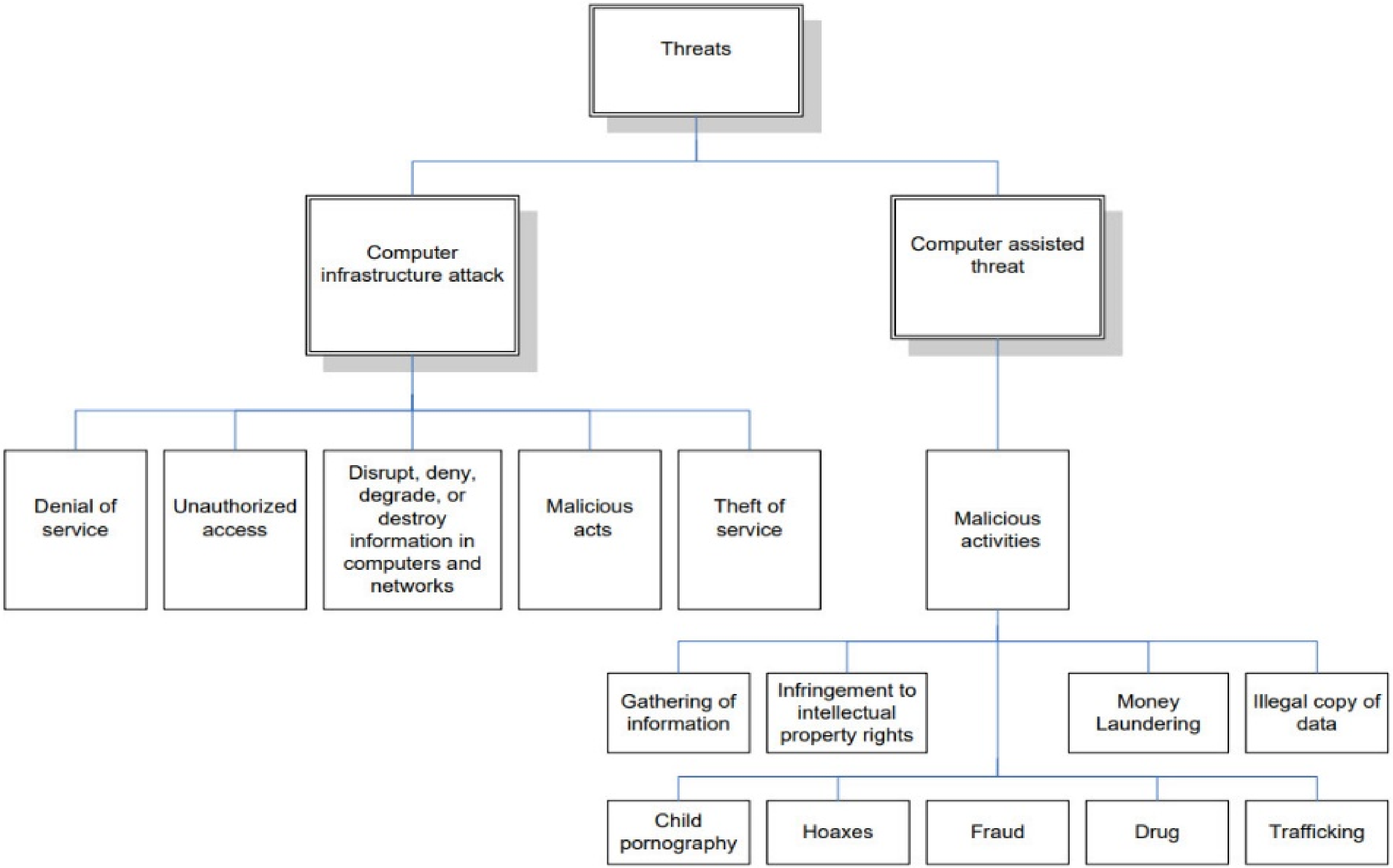
Unauthorized access to computer systems and service

Unauthorized reproduction of legally protected computer programs

The CoE taxonomy of cybercrime offences


Cybercrime Offences
Offences against confidentiality, integrity, and availability of computer systems and data.
Computer related offences
Content related offences
Offences related to infringements of copyright and related rights
Illegal access
Illegal interception
Data interference
System interference
Misuse of Devices
Forgery
Fraud
Child pornography

The G8 taxonomy of threats



Threats

Computer infrastructure attack

Computer assisted threat

Denial of service

Unauthorized access

Disrupt, deny, degrade, or destroy information in computers and networks

Malicious acts

Theft of service

Malicious activities

Gathering of information

Infringement to intellectual property rights

Money Laundering

Illegal copy of data

Child pornography

Hoaxes

Fraud

Drug

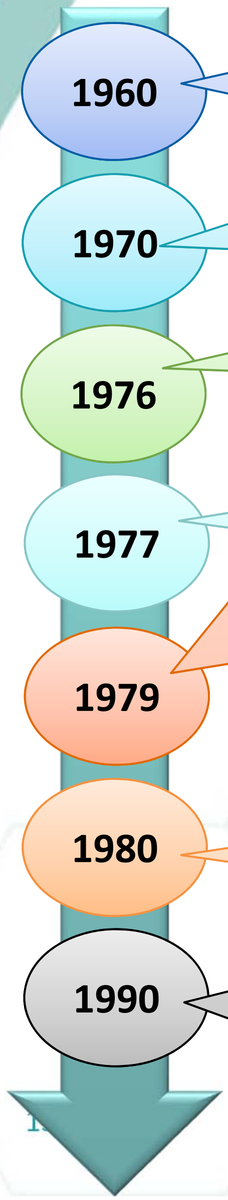
Trafficking

Cybercrime activities

- Hacking and related activities
- Viruses and other malicious programs
- Fraud and Theft
- Gambling, Pornography and other offences against morality
- Child pornography and other offences against minors
- Stalking, Harassment, Hate speech
- Other offences against persons
- Cyberterrorism

A BRIEF CHRONOLOGY: NATIONAL AND INTERNATIONAL EFFORTS

THE ORIGINS OF COMPUTER CRIME AND NATIONAL LEGISLATION: 1960'S-1970'S



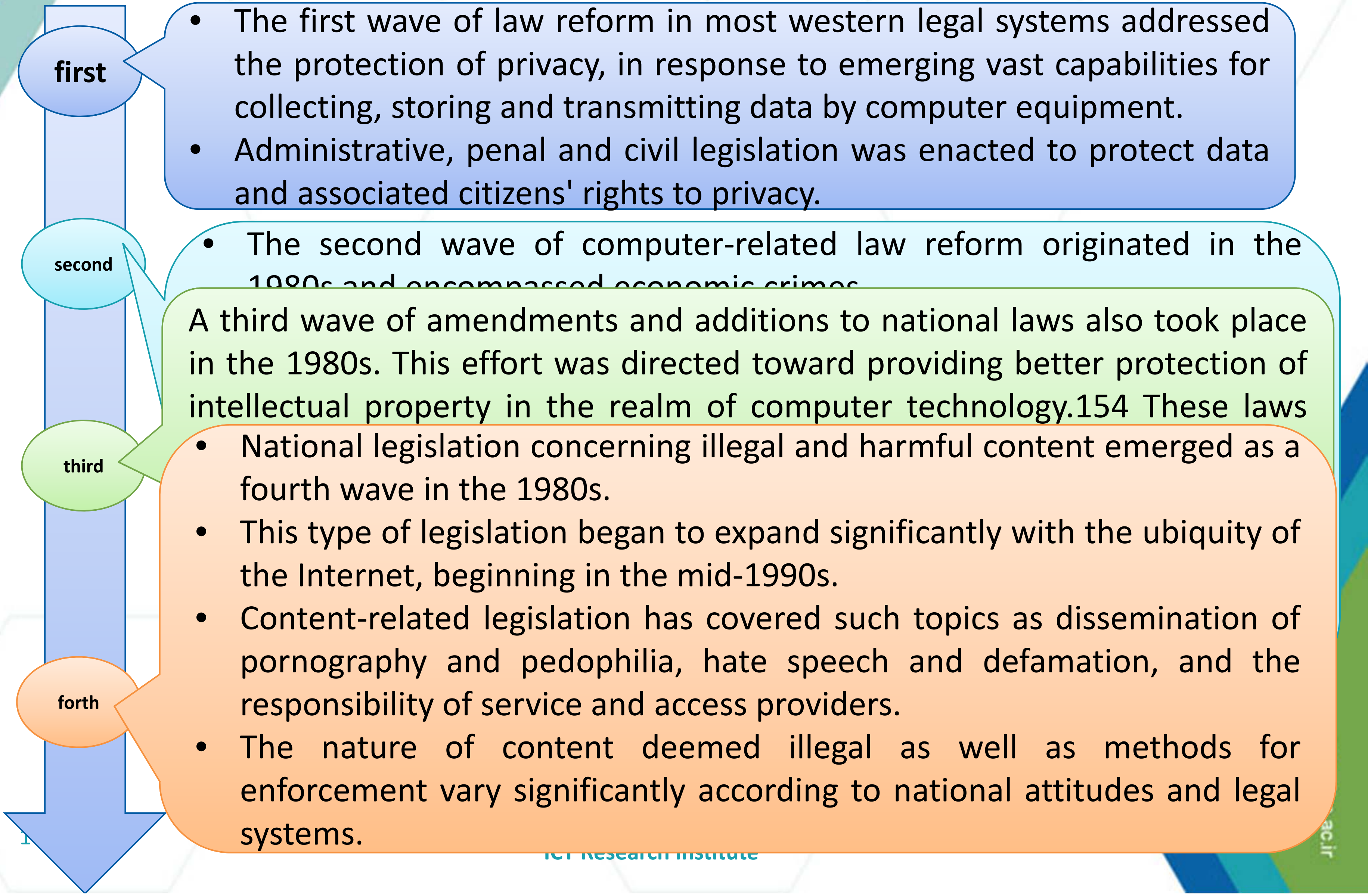
- The first published accounts of computer manipulation, sabotage, espionage, and the illegal use of computer systems.

- The first empirical computer crime studies to apply criminological research methods

- The bill, revised and reintroduced, declared
  - any "knowing, willful manipulation or attempted manipulation: of "any computer owned or operated by the United States, certain financial institutions, and entities affecting interstate commerce, for the purpose of `devising or executing any scheme or artifice to defraud,' or of `obtaining money, property, or services...by means

- Vulnerabilities of an information-based society and limitations of existing computer security approaches, as well as the limitations of law and enforcement efforts were widely publicized in the 1990s.
- Computer crime has expanded in scope far beyond mere economic crime, and can be expected to include attacks against national infrastructure, security and social well being.

THE MAIN WAVES OF NATIONAL LEGISLATION: 1970'S-1990'S



first

- The first wave of law reform in most western legal systems addressed the protection of privacy, in response to emerging vast capabilities for collecting, storing and transmitting data by computer equipment.
- Administrative, penal and civil legislation was enacted to protect data and associated citizens' rights to privacy.

second

- The second wave of computer-related law reform originated in the 1980s and encompassed economic crimes

third

A third wave of amendments and additions to national laws also took place in the 1980s. This effort was directed toward providing better protection of intellectual property in the realm of computer technology.154 These laws

forth

- National legislation concerning illegal and harmful content emerged as a fourth wave in the 1980s.
- This type of legislation began to expand significantly with the ubiquity of the Internet, beginning in the mid-1990s.
- Content-related legislation has covered such topics as dissemination of pornography and pedophilia, hate speech and defamation, and the responsibility of service and access providers.
- The nature of content deemed illegal as well as methods for enforcement vary significantly according to national attitudes and legal systems.

CHRONOLOGY OF INTERNATIONAL EFFORTS

1983

In 1983, a group of experts met and recommended that the OECD take the initiative in trying to achieve the harmonization of European computer crime legislation.

1983-1985

From 1983 to 1985, the OECD carried out a study of the possibility of an international application and harmonization of criminal laws to address cybercrime and abuse.

1986

The study resulted in the 1986 report *Computer-related Crime: Analysis of Legal Policy*, which surveyed existing laws and proposals for reform and recommended a minimum list of abuses that countries should consider criminalizing.

1985-1989

From 1985 to 1989, the Select Committee of Experts on Computer-Related Crime of the Council of Europe discussed the issues raised by cybercrime and drafted Recommendation 89(9), adopted September 13, 1989.

1990

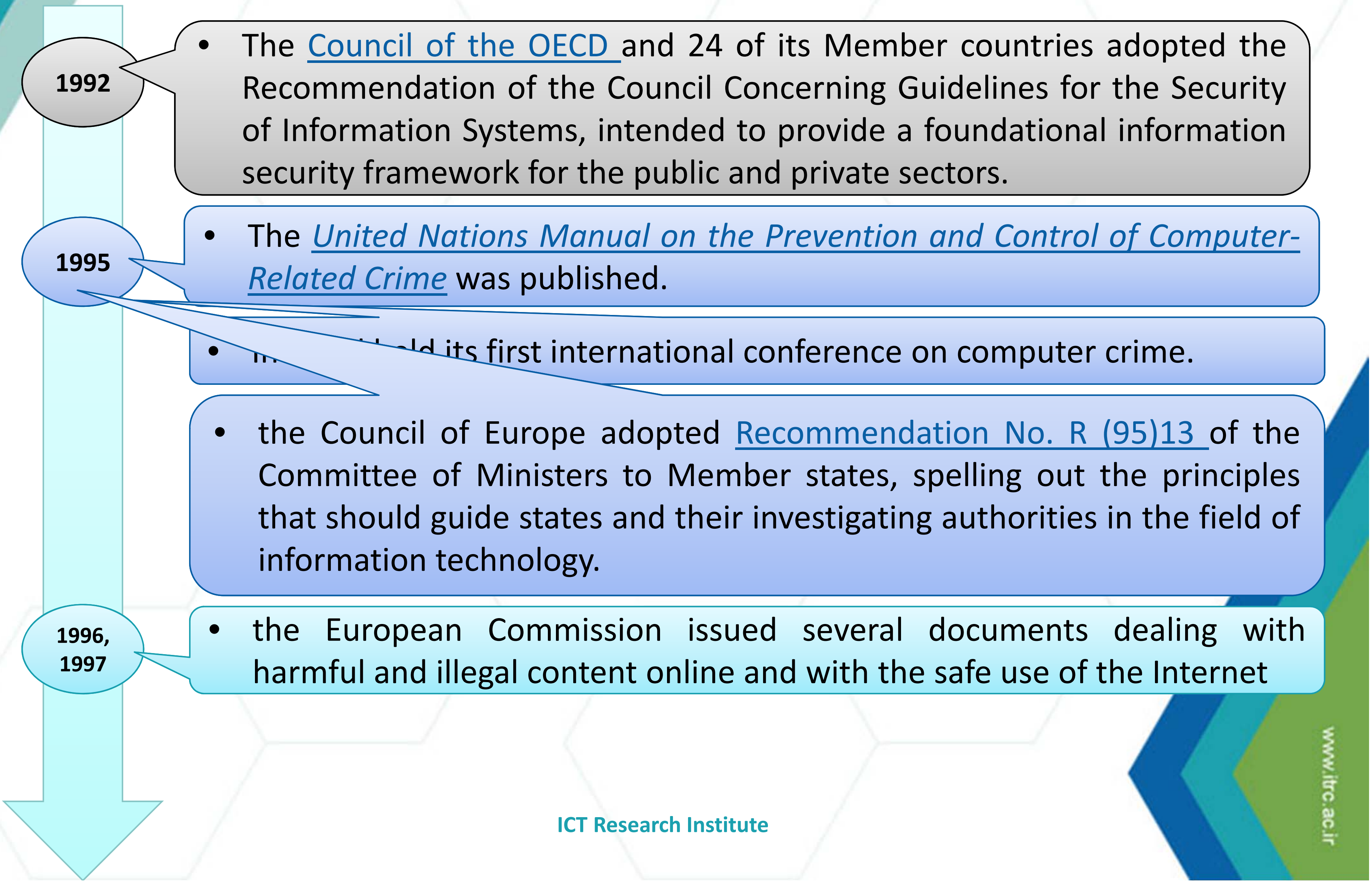
The Eighth United Nations Congress on the Prevention of Crime and the

[illegible]

appropriate legislation and policy directives.” The
General Assembly adopted this resolution on December 14, 1990.

- The first Interpol working party, the European Working Party on Information Technology Crime, was established.

CHRONOLOGY OF INTERNATIONAL EFFORTS



1992

- The Council of the OECD and 24 of its Member countries adopted the Recommendation of the Council Concerning Guidelines for the Security of Information Systems, intended to provide a foundational information security framework for the public and private sectors.

1995

- The *United Nations Manual on the Prevention and Control of Computer-Related Crime* was published.

- In[illegible] held its first international conference on computer crime.

- the Council of Europe adopted Recommendation No. R (95)13 of the Committee of Ministers to Member states, spelling out the principles that should guide states and their investigating authorities in the field of information technology.

1996, 1997

- the European Commission issued several documents dealing with harmful and illegal content online and with the safe use of the Internet

CHRONOLOGY OF INTERNATIONAL EFFORTS

1997

- the European Parliament adopted a resolution on the European Commission's "communication on illegal and harmful content on the Internet, supporting the initiatives undertaken by the Commission and stre ed for international co-operation in various areas.

- and Interior Ministers of the Group of Eight199 (G8) met in lopted ten Principles to Combat High-Tech Crime.

- t Directorate for Science, Technology and Industry directed a fiv w of the progress that had been made toward impl 1992 *Guidelines for the Security of Information System* e.

- The Council of Europe's European Committee on Crime Problems (CDPC)

- The G8 held a cybercrime conference to discuss "how to jointly crack

2000

In June of 2000, an Action Plan prepared by the European Commission and the European Council was adopted by the Feira Summit of the European Council.

2001

- The Parliamentary Assembly of the Council of Europe approved the Draft Convention on Cyber Crime at its April, 2001 session, and it was opened for signature by the member states on November 23, 2001.

Computer-related Crime: Analysis of Legal Policy

- This list was compiled as a result of a comparative analysis of substantive law around the world and outlined commonly recognized acts, which could constitute a shared basis for the different approaches taken by member states:
  1) The input, alteration, erasure and/or suppression of computer data and/or computer programs made wilfully with the intent to commit an illegal transfer of funds or of another thing of value;
  2) The input, alteration, erasure and/or suppression of computer data and/or computer programs made wilfully with the intent to commit a forgery;
  3) The input, alteration, erasure and/or suppression of computer data and/or computer programs, or other interference with computer systems, made wilfully with the intent to hinder the functioning of a computer and/or of a telecommunication system;
  4) The infringement of the exclusive right of the owner of a protected computer program with the intent to exploit commercially the program and put it on the market;
  5) The access to or the interception of a computer and/or telecommunication system made knowingly and without the authorization of the person responsible for the system, either by infringement of security measures or for other dishonest or harmful intentions.

Recommendation 89(9)

- Recommendation 89(9) emphasized the importance of an adequate and quick response to cybercrime, the transborder nature of which requires harmonization of law and practice and improved international legal cooperation.

- It further emphasized the need for international consensus in criminalizing and addressing certain computer-related offenses.

The Council of the OECD effort

- The *Guidelines for the Security of Information Systems* were annexed to the Recommendation.
- This framework includes laws, codes of conduct, technical measures, management and user practices, and public education provisions.
- The *Guidelines* focus on the implementation of minimum standards for the security of information systems.
- In parallel, however, the *Guidelines* request that Member States establish adequate penal, administrative or other sanctions for misuse of information systems, and develop means for mutual assistance, extradition and other international cooperation in matters of security of information systems.

United Nations Manual on the Prevention and Control of Computer-Related Crime Manual

- The *Manual* examines the phenomenon of computer crime, substantive criminal law protecting
  - the holder of data and information,
  - substantive criminal law protecting privacy,
  - procedural law,
  - crime prevention in the computer environment, and
  - the need for and avenues to international cooperation.

Recommendation No. R (95)13

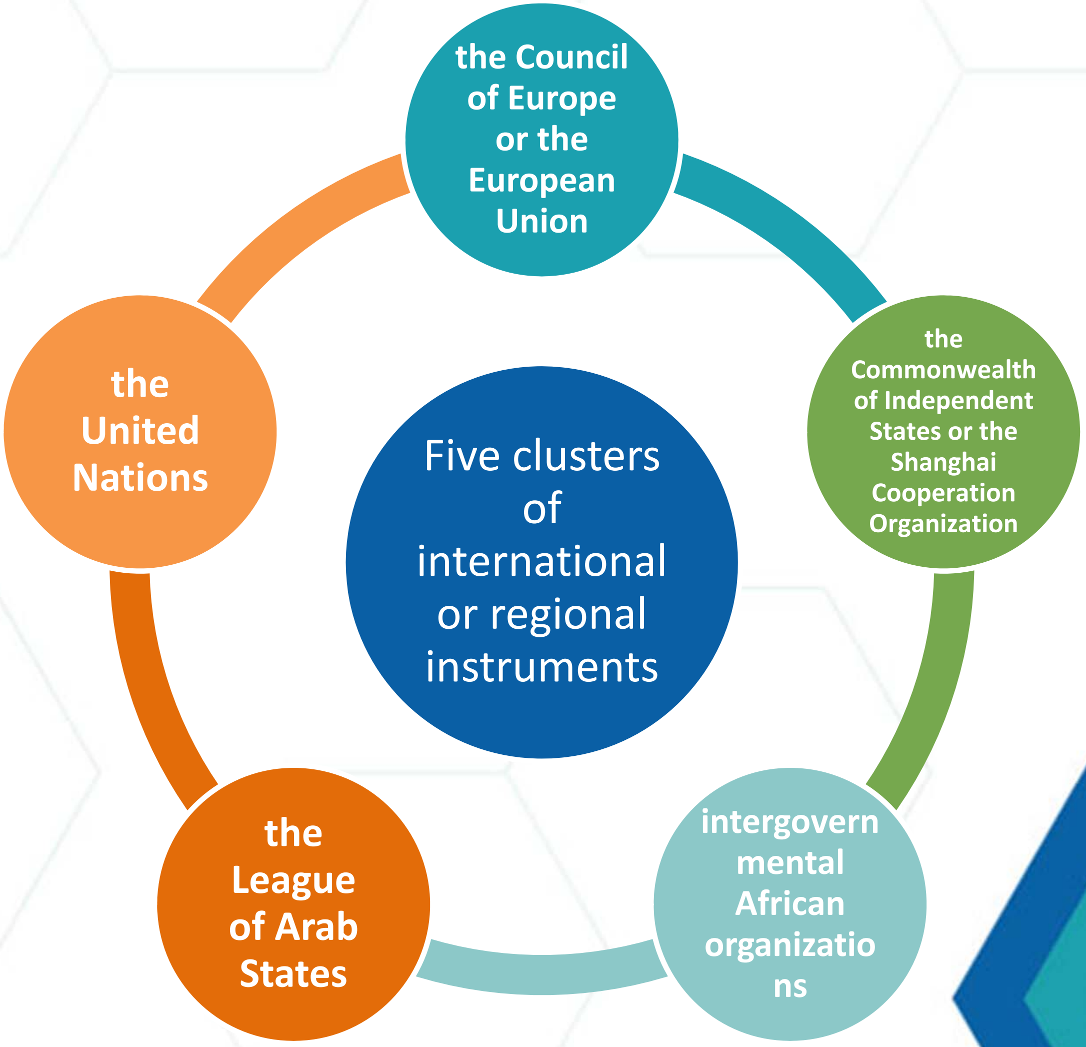
- The principles cover
  - search and seizure,
  - Technical surveillance,
  - obligations to co-operate with the investigating authorities,
  - electronic evidence,
  - use of encryption, research, statistics
  - and training, and international cooperation.

- The document addresses these issues from the perspectives of investigating both cybercrime and traditional crimes where evidence may be found or transmitted in electronic form.

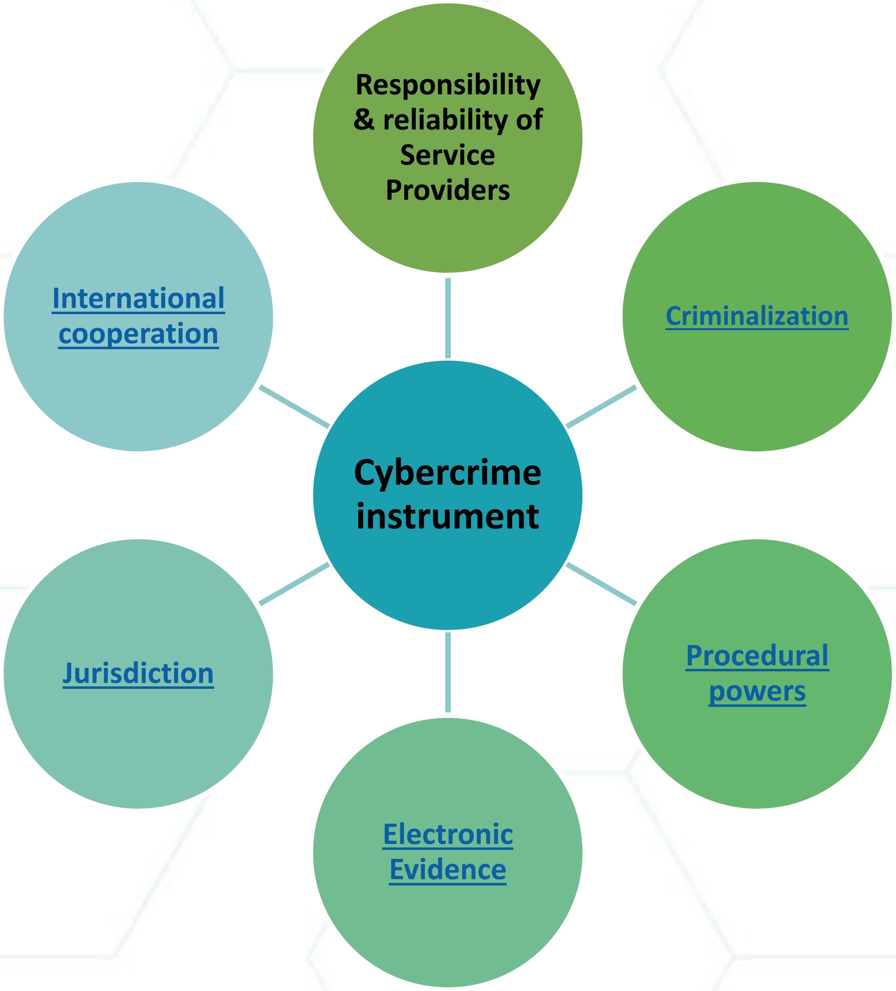
Legislation and framework

Five clusters of international or regional instruments

A significant amount of cross-fertilization exists between all instruments, including, in particular, concepts and approaches developed in the Council of Europe Cybercrime Convention


Five clusters of international or regional instruments
the Council of Europe or the European Union
the Commonwealth of Independent States or the Shanghai Cooperation Organization
intergovernmental African organizations
the League of Arab States
the United Nations

Substantative focus of cybercrime instruments



Criminalization

- The principle of nullum crimen sine lege (no crime without law) requires that the conduct constituting any criminal offence must be described clearly by law.

Criminalization

An understanding of criminalization approaches used, and differences between national criminal laws in the area of cybercrime, is important for three reasons.

Firstly, criminalization *gaps* in any country can create offender havens with the potential to affect other countries globally.

Secondly, criminalization *differences* introduce challenges for effective international cooperation in criminal matters involving cybercrime – in particular, as regards the principle of dual criminality.

Thirdly, a comparative analysis of cybercrime offences is able to explore *good practice* that states may use in the development of national laws, in accordance with emerging international standards in this area.

Criminalization

- **An analysis of criminalization acts by UNDOC shows that**
  - **'Core' cybercrime acts** against the
    - confidentiality,
    - integrity and
    - accessibility of computer systems

    are criminalized in many countries using **cyber-specific offences**.

  - **Computer-related acts**, such as those involving
    - breach of privacy,
    - fraud or forgery, and
    - identity offences,

    are more often criminalized using **general offences**.

Procedural powers

- An effective investigation of crime is not possible without adequate investigative powers.

- Due to their often intrusive nature, such measures must be regulated by law and accompanied by adequate safeguards.

- Specialized powers are therefore required, such as
  - for the **gathering** of electronically stored and communicated computer content,
  - for the **identification and localization** of computer devices and communications,
  - for the quick ‘**freeze**’ of volatile computer data,
  - and for ‘**undercover**’ online investigations.

Gathering and using evidence

- Traditional criminal procedural law typically contains provisions on the gathering and admissibility of evidence.

- When it comes to evidence in electronic form, **computer data can be altered easily**.

- Thus, the gathering and handling of electronic evidence must guarantee the
  - integrity,
  - authenticity and
  - continuity of evidence

  during the entire time period between its seizure and its use in trial – a process often known as the '**chain of custody**.'

Jurisdiction and international cooperation

- More than half of responding countries reported that between 50 and 100 percent of cybercrime acts encountered by police involved a ‘transnational element.’

- The prosecution of transnational acts requires states to assert two types of ‘jurisdiction’, both substantive and investigative.
  - Firstly, states must be able to assert that their national criminal law applies to an act that takes place only partly, or even not at all, within its national territory.
  - Secondly, states need to be able to carry out investigative actions that concern the territory of other states.

Law enforcement and cybercrime

- The role of law enforcement
  - Article 1 of the United Nations Code of Conduct for Law Enforcement Officials highlights that the role of law enforcement is to fulfil the duty imposed upon them by law, ***'by serving the community'* and *'by protecting all persons against illegal acts*.'**
  - As cybercrime acts become ever more prevalent, law enforcement agencies increasingly face the question of what it means to
    - 'serve' and
    - 'protect'

    in the context of a crime with global dimensions.

ELECTRONIC EVIDENCE AND CRIMINAL JUSTICE

- Evidence is the means by which facts relevant to the guilt or innocence of an individual at trial are established.
- Electronic evidence is all such material that exists in electronic, or digital form.
- Digital forensics is concerned with recovering – often volatile and easily contaminated –information that may have evidential value.
- Forensics techniques include the creation of 'bit-for-bit' copies of stored and deleted information, 'write-blocking' in order to ensure that original information is not changed, and cryptographic file 'hashes,' or digital signatures, that can demonstrate changes in information.

ELECTRONIC EVIDENCE AND CRIMINAL JUSTICE

- Legal frameworks optimized for electronic evidence, together with law enforcement and criminal justice capacity to
  - identify,
  - collect and
  - analyze electronic evidence,

  are thus central to an effective crime response.

- There are two important topics in this field in different countries:
  - The **capacity of law enforcement authorities** and prosecutors to collect and handle electronic evidence.
  - Legal frameworks for electronic evidence, including admissibility and evidentiary laws and rules that apply to electronic evidence.

INTERNATIONAL COOPERATION

- A ‘transnational dimension’ to a cybercrime offence arises where an element or substantial effect of the offence is another territory, or where part of the *modus operandi* of the offence is in another territory.

International legal assistance regimes

- There are different treaties in international cooperation:

‘extradition’ treaties

- Extradition can be defined as the formal process whereby a state requests the enforced return of a person accused or convicted of a crime to stand trial or serve a sentence in the requesting state.

mutual legal assistance

- the core tools of international cooperation include the provision of assistance in gathering evidence for use in criminal cases and arrangements for the international transfer of sentenced persons.
- the procedure to be followed in processing both incoming and outgoing requests is often set out in national law.

***Informal* police-to-police communicatio n:**

- parts of the process of extraterritorial law enforcement investigations may be undertaken by *informal* police-to-police or agency-to-agency communication.
- Such communication can be used *prior* to a formal mutual legal assistance request to a competent authority, or to *facilitate* a formal request.

What is a ‘transnational dimension’?

- the United Nations Organized Crime Convention – which provides that an offence is ‘*transnational in nature*’ if:

it is committed in more than one state;

it is committed in one state but a substantial part of its preparation, planning, direction or control takes place in another state;

it is committed in one state but involves an organized criminal group that engages in criminal activities in more than one state; or

it is committed in one state but has substantial effects in another state.

PREVENTION

‘Crime prevention’ refers to the strategies and measures that seek to reduce the *risk* of crimes occurring, and their potential harmful effects on individuals and society, through interventions that influence the multiple causes of crime.

The United Nations Guidelines for the Prevention of Crime highlight that government leadership plays an important part in crime prevention, combined with cooperation and partnerships across ministries and between authorities, community organizations, non-governmental organizations, the business sector and private citizens.

- **Good crime prevention practice starts with basic *principles* (such as leadership, cooperation, and the rule of law),**
  - **suggests forms of *organization* (such as crime prevention plans), and**
  - **leads to the implementation of *methods* (such as development of a sound knowledge base) and**
  - ***approaches* (including reducing criminal opportunities and target hardening).**

Council of Europe Convention on Cybercrime

- In 2001, realizing that certain computer-related offenses required special consideration, 26 member countries convened in Budapest and signed the Council of Europe Convention on Cybercrime to create "a common criminal policy aimed at the protection of society against cybercrime, *inter alia*, by adopting appropriate legislation and fostering international cooperation"

- The Convention on Cybercrime entered into force on July 1, 2004, and its status as of January 22, 2009, is that it has been signed by 46 States and ratifed by 23, including the United States of America (as a nonmember state of the CoE), where it entered into force on January 1, 2007, and the Netherlands, where it entered into force on March 1, 2007.

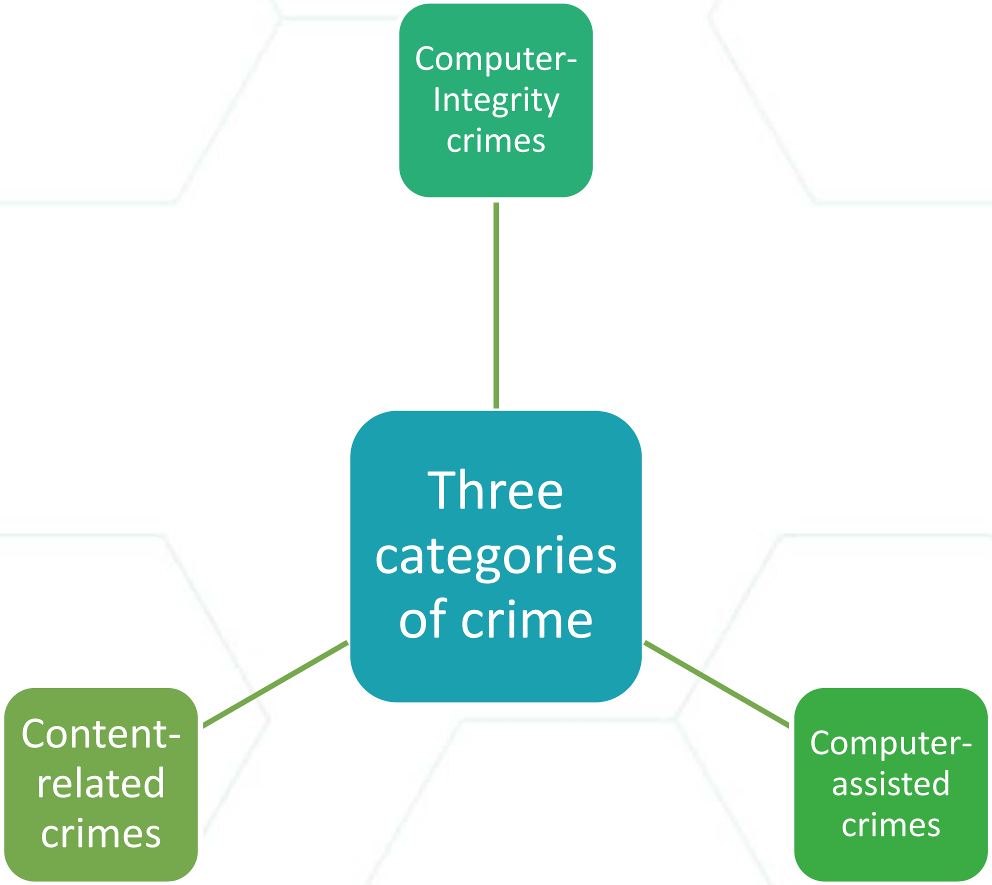
- It has been signed but not yet ratifed by Ireland and the United Kingdom. Thus, it does not have legal effect in those jurisdictions.

Scope of cybercrime convention

- Substantial criminal law (criminal offences to be established under domestic law)
- Procedural law (six procedural powers to be established under domestic law)
- Rules on international co-operation

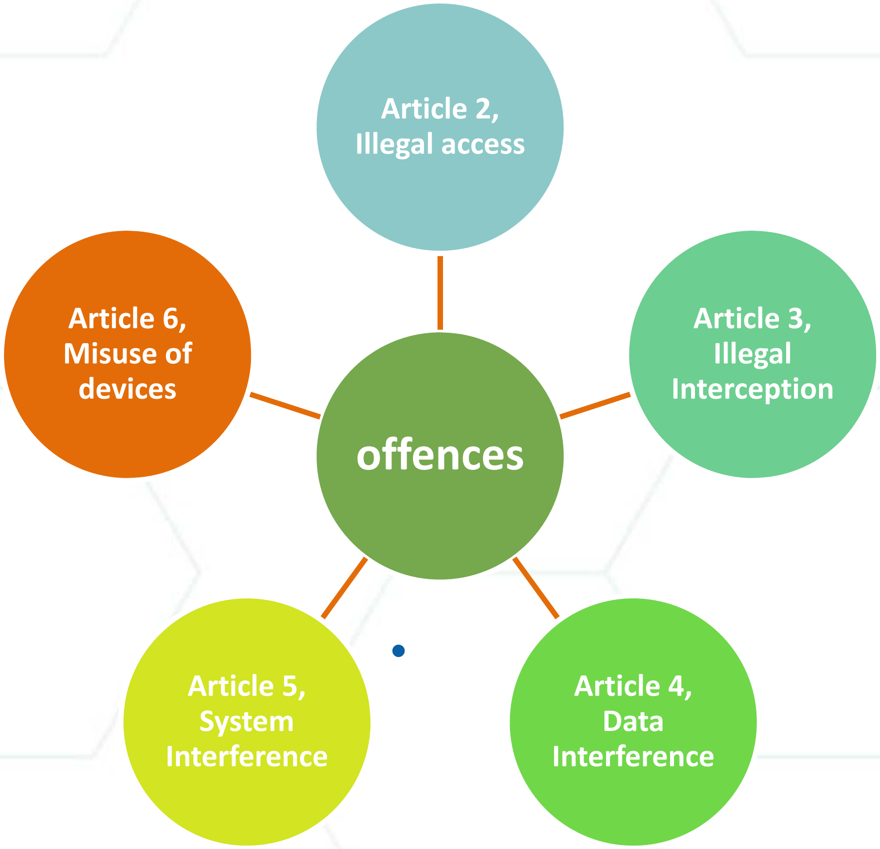
- **Substantive criminal law**
- **Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems**

SPECIFIC CyBERCRIME OFFENSES

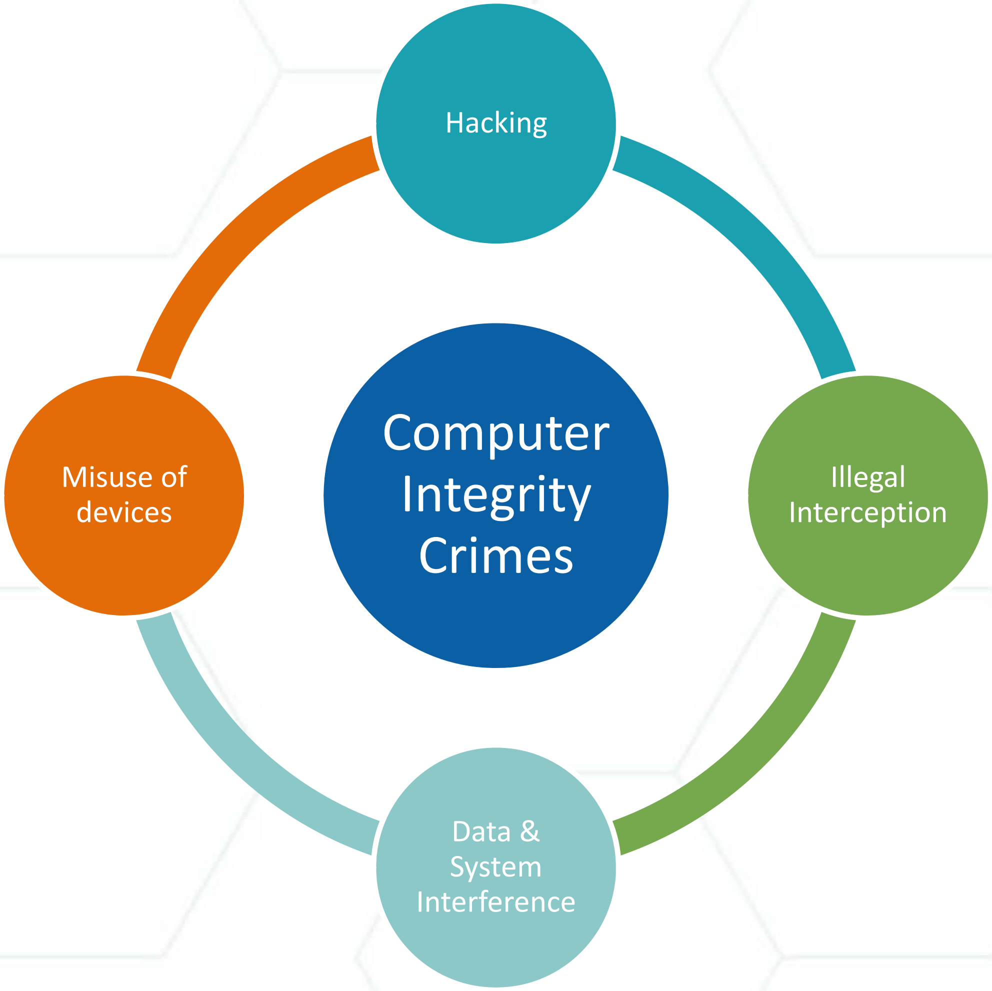


Computer-Integrity Crimes

- The Council of Europe Convention on Cybercrime introduces the following five offenses against the confidentiality, integrity, and availability of computer data and systems:



COMPuTER-INTEGRITy CRIMES



Computer Integrity Crimes

Hacking

Illegal Interception

Data & System Interference

Misuse of devices

COMPUTER-ASSISTED CRIMES

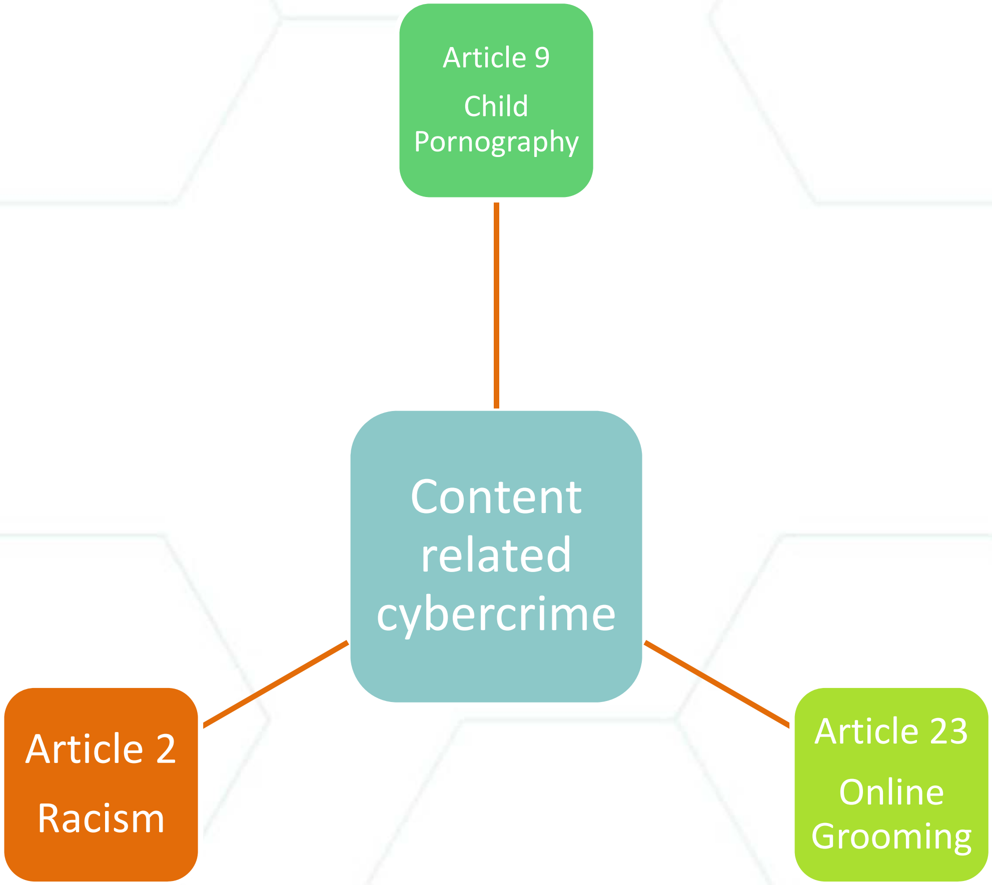
Forgery

- Art. 7 of the Cybercrime Convention criminalizes computer-related forgery : the intentional and unlawful “input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible.” Parties may pose a requirement of dishonest intent.

Fraud

- “causing of a loss of property to another person by [interfering with computer data or a computer system] with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person”
- The Fraud Act of 2006 updated the law in England. Section 2 sets out the offence of fraud

CONTENT-RELATED CYBERCRIMES



Content related cybercrime

Article 9

Child Pornography

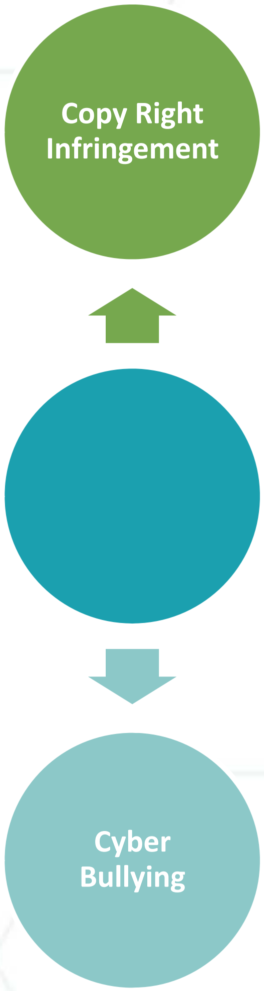
Article 2

Racism

Article 23

Online Grooming

OTHER OFFENSES



Convention on Cybercrime: Section 2

Article 16: Expedited preservation of stored computer data

Article 17: Expedited preservation and partial disclosure of traffic data

Article 18: Production order

Article 19: Search & seizure of stored computer data

Article 20: Real-time collection of traffic data

Article 21: Interception of content data

Article 15: Conditions & Safegaurds

Procedural powers necessary to detect, investigate and prosecute cybercrime

Necessary to safeguard human rights and freedoms

Rules on international co-operation – Section 3

- **Jurisdiction:**
- Jurisdiction in cybercrimes is a tricky issue.
- Acts on the Internet that are legal in the state where they are initiated may be illegal in other states, even though the act is not particularly targeted at that particular state.
- Jurisdiction has several forms:
  - jurisdiction to prescribe: the authority of a sovereign “to make its law applicable to the activities, relations, or status of persons, or the interests of persons in things by legislation, by executive act or order, by administrative rule or by determination of a court
  - jurisdiction to adjudicate,
  - and jurisdiction to enforce.

Major constituting factors of jurisdiction in cybercrime

- **Location**: is therefore a primary constitutive factor for jurisdiction, even with cybercrimes.
- **Indirect links**: Some countries even go so far as to claim jurisdiction on the basis of very indirect links with their territory.
- **Nationality of the perpetrator:** is the second major constituting factor of jurisdiction in cybercrime

Loop holes and need to update

International Consensus

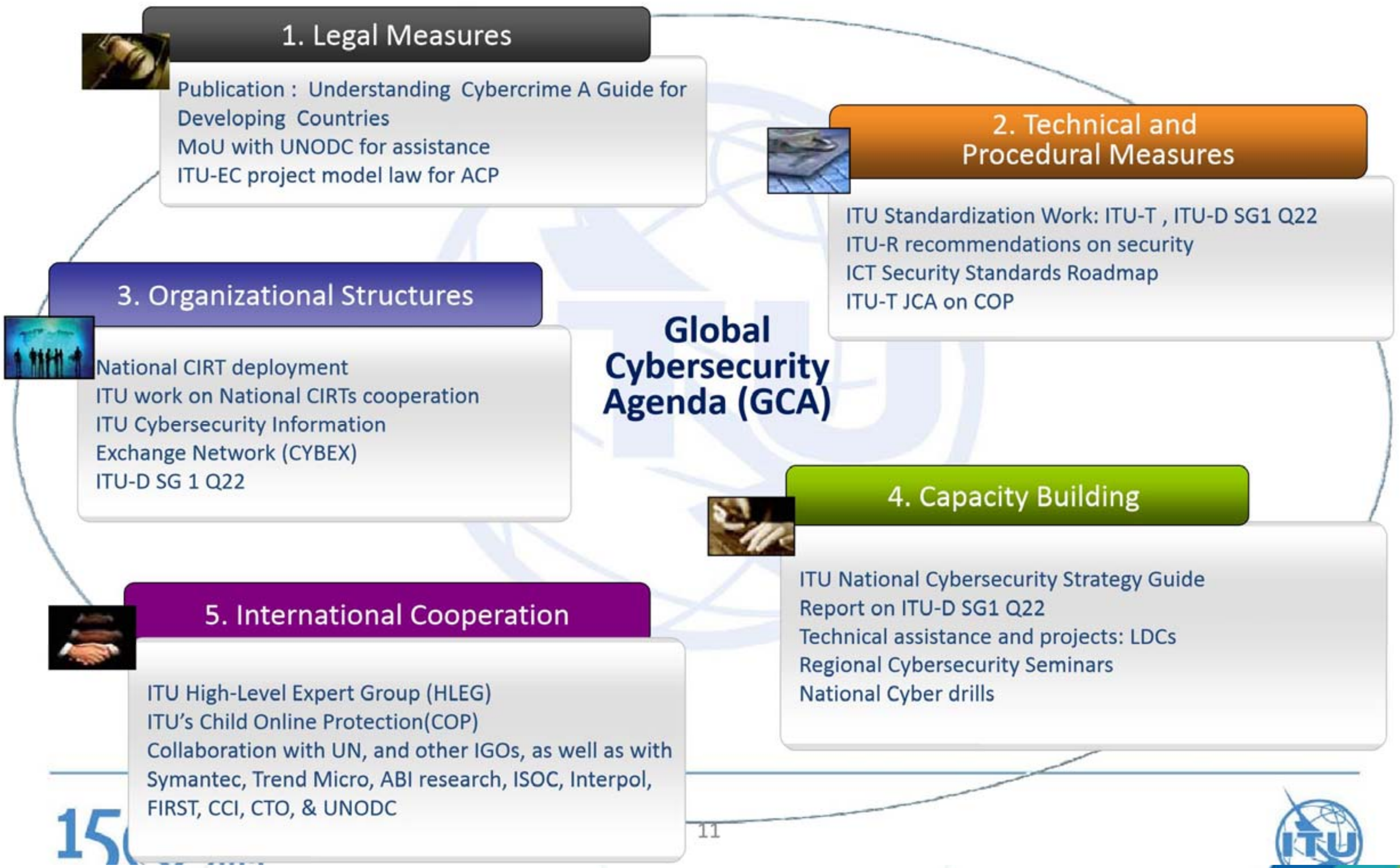
- Two areas in which some level of consensus is necessary if law enforcement and judicial actors working from within various national jurisdictions are to be effective in identifying, investigating and prosecuting computer offenses.
  - The first area is that of specifying what conduct will be treated as a criminal offense. Because this area shows the most potential for formal agreement in the short term, it is the main focus of the Draft Convention.
  - The second area concerns points of existing consensus on what rules and procedures should dictate the scope and extent of operational powers enjoyed by law enforcement and judicial authorities inside their respective spheres of jurisdiction.
- **International law enforcement and judicial cooperation depend upon at least general agreement on what conduct should be regarded as punishable offenses.**
- In practice, this principle also extends to mutual legal assistance in gathering evidence in the course of a criminal investigation, particularly when the acts of discovery in question are considered intrusive.

Administration and Operation of Cyber Law

- As difficult as reaching consensus on issues of substantive law appears to be, the difficulties multiply when the discussion turns to administration and procedure.
- that the scenario could be easily complicated by the addition of other common considerations, notably
  - the number of nations involved,
  - the presence or absence of extreme urgency,
  - the existence of consent and its voluntariness, and
  - the extent to which the data sought is protected by firewalls, passwords or encryption.

ITU works on cybersecurity

ITU Global Cybersecurity Agenda



Global Cybersecurity Agenda (GCA)

1. Legal Measures
- Publication : Understanding Cybercrime A Guide for Developing Countries
- MoU with UNODC for assistance
- ITU-EC project model law for ACP

2. Technical and Procedural Measures
- ITU Standardization Work: ITU-T , ITU-D SG1 Q22
- ITU-R recommendations on security
- ICT Security Standards Roadmap
- ITU-T JCA on COP

3. Organizational Structures
- National CIRT deployment
- ITU work on National CIRTs cooperation
- ITU Cybersecurity Information Exchange Network (CYBEX)
- ITU-D SG 1 Q22

4. Capacity Building
- ITU National Cybersecurity Strategy Guide
- Report on ITU-D SG1 Q22
- Technical assistance and projects: LDCs
- Regional Cybersecurity Seminars
- National Cyber drills

5. International Cooperation
- ITU High-Level Expert Group (HLEG)
- ITU's Child Online Protection(COP)
- Collaboration with UN, and other IGOs, as well as with Symantec, Trend Micro, ABI research, ISOC, Interpol, FIRST, CCI, CTO, & UNODC

11

- The Global Cybersecurity Index (GCI) aims to measure the level of commitment of each nation in cybersecurity in five main areas:
  - Legal Measures
  - Technical Measures
  - Organizational Measures
  - Capacity Building
  - National and International Cooperation

Legal measures

- Within the five pillars the legal measure are probably the most relevant with regard to an Anti-Cybercrime Strategy.
- The requirements:
  - This requires first of all the necessary substantive criminal law provisions to criminalize acts such as computer fraud, illegal access, data interference, copyright violations and child pornography.
  - Apart from substantive criminal law provisions, the law enforcement agencies need the necessary tools and instruments to investigate cybercrime.
    - Perpetrators can act from nearly any location in the world and take measures to mask their identity.
    - The tools and instruments needed to investigate cybercrime can be quite different from those used to investigate ordinary crimes.

Technical and Procedural Measures

- Cybercrime-related investigations very often have a strong technical component.
  - In addition the requirement of maintaining the integrity of the evidence during an investigation requires precise procedures.
  - Another issue is the development of technical protection systems.
    - Well-protected computer systems are more difficult to attack.
    - Improving technical protection by implementing proper security standards is an important first step.

Organizational Structures

- An effective fight against cybercrime requires highly developed organizational structures.
- Without having the right structures in place that avoids overlapping and is based on clear competences it will hardly be possible to carry out complex investigations that require the assistance of different legal as well as technical experts.

Capacity Building and User Education

- In order to be able to effectively investigate offences harmonization of laws and the development of means of international cooperation needs to be established.
- In order to ensure global standards in developed countries as well as in developing countries **capacity building** is necessary.
- In addition to capacity building **user education** is required.
  - Certain cybercrimes – especially those related to fraud, such as "phishing" and "spoofing" – do not generally depend on a lack of technical protection, but rather lack of awareness by victims.
  - There are various software products that can automatically identify fraudulent websites, but until now, these products cannot identify all suspicious websites.
  - One of the most important elements in the prevention of cybercrime is user education.
  - One important requirement of an efficient education and information strategy is the open communication of the latest cybercrime threats.

International Cooperation

- In a large number of cases data transfer processes in the Internet affect more than one country.
- This is a result of the design of the network as well as the fact the protocols that ensures that successful transmissions can be made, even if direct lines are temporarily blocked.
- In addition a large number of Internet services (like for example hosting services) are offered by companies that are based abroad.
- In those cases where the offender is not based in the same country at the victim, the investigation requires cooperation between law enforcement agencies in all countries that affected. International and transnational investigations without the consent of the competent authorities in the countries involved are difficult with regards to the principle of National Sovereignty.
- This principle does in general not allow one country to carry out investigations within the territory of another country without the permission of the local authorities.
- Therefore, investigations need to be carried out with the support of the authorities in all countries involved.

ITU ACTIVITIES ON STRENGTHENING THE ROLE OF ITU IN BUILDING CONFIDENCE AND SECURITY IN THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES

1- Legal Measures

ITU is assisting Member States in understanding the legal aspects of cybersecurity through its ITU Cybercrime Legislation Resources in order to help harmonize their legal frameworks.

In the area of legal measures, ITU collaborates closely with partners such as UNODC and others that may have expertise in this area.

2- Technical and Procedural Measures

ITU Technical and Procedural Measures	ITU-T Study Group 17 (SG-17), the lead study group on security and identity management (IdM), continues to be instrumental in study and standardization in the areas of cybersecurity, anti-spam, IdM, ITU-T X.509 certificates, information security management, ubiquitous sensors networks, telebiometrics, mobile security, virtualization security towards cloud computing security, personally identifiable information protection and security architecture and application security, often in cooperation with external Standards Developing Organizations and Consortia.
	ITU-T SG17 agreed to establish a new Question 14/17 on “Security Aspects of Distributed Ledger Technologies” and approved new Recommendations
	An ITU Workshop on Security Aspects of Blockchain was held on 21 March 2017, in Geneva, Switzerland to examine Blockchain’s potential in enhancing trust in the use of ICTs.
	ITU SG17 organized an ITU Workshop on Security Aspects of Intelligent Transport Systems
	The ITU SG17 Regional Group for Arab Region held its first meeting on 10 December 2017
	ITU SG17 plans to organize an ITU workshop on 5G Security on 19 March 2018
	ITU SG17 continued coordination with ITU-T SG20 “IoT and its applications including smart cities and communities (SC&C)” on IoT security.
	ITU-R’s work in radiocommunication standardization continues, matching the constant evolution in modern telecommunication networks.

3- Organizational Structures

ITU continues to help build capacity at regional and international levels. ITU has undertaken technical assessments to evaluate the preparedness for the establishment of Computer Incident Response Teams (CIRTs) in 68 countries and is continuing with the necessary follow-up actions.

ITU partnered with the Global Cyber Security Capacity Centre at the Oxford Martin School, and jointly performed Cybersecurity Capacity Reviews in Thailand, Sierra Leone, and Madagascar.

A National Cybersecurity Strategy toolkit is under development, as a multistakeholder effort facilitated by ITU.

4- Capacity Building

ITU continues to organize regional cybersecurity forums for all ITU regions, using them as a capacity-building vehicle for different BDT programmes and activities as well as an operational platform for cooperation at the regional and international level.

Following WTDC 2017, Question 3/2 (Securing information and communication networks: Best practices for developing a culture of cybersecurity) will continue its work during study period 2018-2021.

ITU, together with the AfricaCERT, organized a five-day capacity-building workshop on "Threat intelligence for CIRTS" on 11-15 December 2017

Following the launch of the first Global Cybersecurity Index (GCI) results in 2014 and its inclusion in Resolution 130 (Rev. Busan, 2014), work was completed on the second version of the Global Cybersecurity Index (GCI) (2017) based on responses from 134 countries, and with the assistance of international partners.

A webinar was organized on 18 December 2017 on the "Report on Global Cybersecurity Index (GCI) for the Europe Region".

An ITU Regional Workshop for Europe and CIS on Cybersecurity and Child Online Protection is planned for 4-6 April 2018

5- International Cooperation

ITU continues to develop relationships and partnerships with various regional and international organizations and initiatives, including the Commonwealth Cybercrime Initiative, ENISA, INTERPOL, ECOWAS, the World Bank, FIRST, and regional CSIRT/CERT associations, such as AP CERT, AFRICA CERT, and OIC CERT.

In its role as the lead facilitator for WSIS Action Line C5, ITU organized several events at the WSIS Forum 2017 that facilitated experience sharing among all stakeholder groups in their global efforts towards building confidence and security in the use of ICTs

ITU participated in the International Multistakeholder Conference "Vienna Cyber Security Week 2018 - Protecting Critical Energy Infrastructure" organized by the Austrian government, EnergyPact Foundation, and the Austrian Institute of Technology, supported by IEC, OSCE and ITU from 29 January to 2 February 2018 in Vienna, Austria.

In IRAN

- CyberCrime Law

- Collection and admissibility of electronic evidence regulation

- Criminal content sample identification committee

- Cyber incident protection and confronting plan

- Maher Center

- Fata Police

Cybercrime Law

- Cybercrime law was enacted at 2010 in Iran.
- It has 56 articles.
- Section 1- crimes and offenses
  - Cybercrimes enacted in this law are as follows, offenses were determined for these crimes
    - Crimes against confidentiality of data, telecommunication and computer systems
    - Crimes against integrity of data, telecommunication and computer systems
    - Computer theft and fraud
    - Crimes against public chastity and morality
    - Distroying dignity and publishing lie
  - It has also determined criminal responsibility of persons and offenses tightening

Cybercrime Law

- Section 2- Procedure of the trial
  - Chapter 1- Competency
  - Chapter 2- Collection of electronic evidence
    - Data retention
    - Immediate preservation of stored computer data
    - Data presentation
    - Search and seizure of data, telecommunication and computer systems
    - Computer communication content intercetion
  - Chapter 3- Admissibility of electronic evidence
- Section 3- Other regulations

Collection and admissibility of electronic evidence regulation

E-COMMERCE
آیین نامهای تجارت الکترونیکی
آیین نامه جمع آوری و استنادپذیری
ادله الکترونیکی
فناوری هوشمند
Fanahoosh.ir
fanahoosh

- The regulation was enacted at 2014 in Iran.
- Collection and admissibility of digital evidence has 48 articles.
  - Section 1- Definitions
  - Section 2- Collection of electronic evidence
    - Data retention
    - Preservation of computer evidence
    - Presentation of computer evidence
    - Search and seizure of computer evidence
  - Other affairs

Criminal content sample identification committee

- This committee was formed based on article 22 of cybercrime law.
- It created a list of criminal contents in 5 sections:
  - Content against public chastity and morality
  - Content against holy beliefs
  - Content against public security and peace
  - Content against public and governmental authorities
  - Cybercriminal contents

Cyber incident protection and confronting plan

- It was enacted at 2017.
- The responsibility of all organizations and authorities to combat cyber incidents was determined in this plan.
- For example,
  - Public cyber incidents are handled by Fata police
  - cyber incidents happening in government organizations are handled by ICT ministry
  - Public electronic evidence are gathered by Fata Police
  - Electronic evidence of government organizations are gathered by national protection organization

Maher Center

مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه ای

- https://www.certcc.ir/
- **Maher Center in Iran cert which is established at 2008.**
- **Its activities are as follows:**
  - **Incident handling and response activities**
    - **Immediate incident handling of government organizations**
  - **Proactive activities**
    - **Disseminating alerts and notifications at national level and protective packages for systems**
  - **activities to improve security level**
    - **Organizing workshops and classes**

FATA Police

- **https://www.cyberpolice.ir/**

The END