CCRIME1

Ivan Acevedo
Information Systems Engineering
Concordia University
Montreal, Canada
i_aceved@encs.concordia.ca

Ali Ahmadi
Information Systems Engineering
Concordia University
Montreal, Canada
al_hmad@encs.concordia.ca

Yunus Emre Aydar
Information Systems Engineering
Concordia University
Montreal, Canada
y_ayda@encs.concordia.ca

Vedant Saini
Information Systems Engineering
Concordia University
Montreal, Canada
v_saini@encs.concordia.ca

Yassine Khalifa
Information Systems Engineering
Concordia University
Montreal, Canada
Y_khal@encs.concordia.ca

Asha Kurugodu
Information Systems Engineering
Concordia University
Montreal, Canada
a_kurug@encs.concordia.ca

Nasim Moghim
Information Systems Engineering
Concordia University
Montreal, Canada
n_moghim@encs.concordia.ca

***Abstract*—By using different technologies and devices, people are facing new problems and crimes. The problem can reach them anywhere and anytime. Cybercrime is one of the mentioned crimes that refers to criminal activity, including internet, computers systems, or networked devices. Most of the cybercrimes are to make profit for the cybercriminals, some of them are accomplished against computers or devices to damage or disable them, while others are used to spread malware, illegal information, images or other materials through using computers or networks.**

A cybercrime can contain many different types of profit-driven criminal activity, including ransomware attacks, email and internet fraud, and identity fraud, so the main purpose of cybercrime activities refers to financial. On the other hand, it tries to steal all kinds of bank account cards information (debit and credit), financial account information, and any types of the payment card information. Sometimes private personal information would be targeted by cybercriminals, as well as theft and resale with the cooperation of data respectively.

Keywords – Cybercrime; cybersecurity; laws; security

I. INTRODUCTION

This project focuses on comparing the different laws related to cybercrime in countries such as Canada, Iran, Turkey, Ecuador, Sweden and South Korea. To find their similarities and differences, as well as to compile computer incidents in which these laws have been violated.

The motivation behind this project is to analyze, from a global perspective, how some countries on different continents of the planet are fighting against cybercrime. Nowadays, there are many international organizations, which try to join efforts to find solutions to cyber-attacks, as well as propose cooperation agreements to ensure the prosperity of nations in the technological field. It is a reality that cybercrime has evolved significantly since its origins. As Grabosky mentions in his book [1], "Cybercrime, in most of its manifestations, has become increasingly sophisticated, both technologically and psychologically". This phenomenon has provided criminals with new tools to carry out more complex computer attacks, whose implications go beyond the simple theft of information or denial of services. Cases such as international networks of child pornography, terrorism, fraud, among others, make use of technological platforms to achieve their goals, therefore, these crimes also become cybercrimes and it is important that each country has an appropriate strategy to combat them. Cybercrime has gone from merely affecting the technological field, to deeper problems involving the social, political and economic global scene.

II. BACKGROUND

CANADA

A. *Legal and Judicial System in Canada*

Being in the northern part of North America, Canada is a parliamentary democracy having ten provinces and three territories. Being a constitutional monarchy in the Westminster tradition, with Elizabeth II as its queen and a prime minister who serves as the chair of the Cabinet and head of government, Canada is officially bilingual at the federal level.

Judicial system of Canada: Canada has its Federal, Provincial and Territorial governments where the federal government pays and appoints judges of the superior courts in all provinces. Forming the Supreme Court of Canada, the Federal Court and the Federal Court of Appeal, as well as the Tax Court, Parliament also has exclusive authority over the procedure regarding to the criminal case tries in those courts. The provinces organize and maintain criminal, civil provincial courts and its procedures. [2]

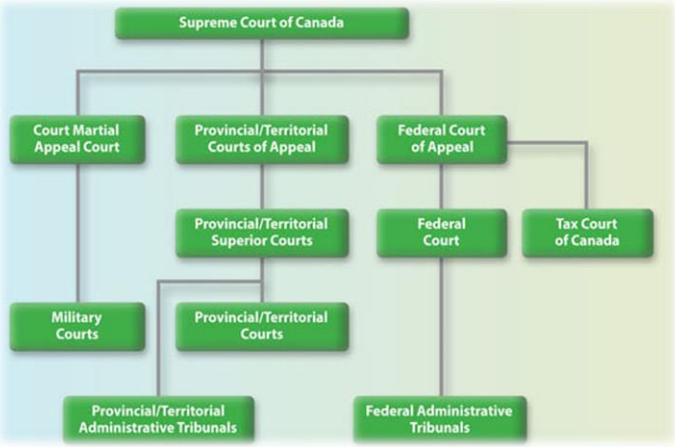


Figure 1: Structure of Judicial System of Canada

Legal System of Canada: Fundamental Principles of Canadian Law reflects the system of Great Britain where laws must be clear and rational, that all accused persons are innocent until proven guilty, that incriminating evidence must meet very high standards, and the law's power over the individual is limited by precedent and the Constitution. Governed by laws, Canadian legal system is how Canada writes, enforces, organizes and interprets laws. Canada evolved politically as a colony of Britain. Canada didn't exist legally until the late 18th Century when Parliaments were set up in the colonies of Canada allowing laws to be written for the first time. Constitution of Canada was created in 1867 when lawmaking power was given to Canada and Canada officially was no longer a colony of Great Britain in 1931. [3]

Types of Laws in Canada are as follows: *Canadian Common Law:* Magna Carta being the cornerstone of Common Law says that government power should be controlled and limited, and that Canadian government must treat aboriginal people with fairness and due process according to the Britain's Royal Proclamation. Specific to each country, common law is the law and corresponding legal system developed through court and tribunal decisions rather than legislative statues or executive action. Judges create and refine them. A case decision currently pending depends on decision of previous case decisions and affects future case decisions.

*Civil Law System***:** Being the opposite of Common law, Civil law system is a Spanish and French tradition of forming extremely precise and specific laws where judges consider situations of an incident. This law tradition is followed by the Quebec Province which was colonized by France, through Charter of Rights and Freedoms to the Canadian Constitution by bringing some common laws into the province too.

The Canadian Charter of Rights and Freedoms: Parliamentary Supremacy begun in 1931 and ever since no authority was considered to be bigger than the Canadian Parliament when they were to decide what is legal and what isn't. All rules passed by Parliament was unquestionably the law until 1982 when Canadian Constitution was formed and sections like Charter of Rights and Freedoms were added. According to Charter, no law passed by Parliament is ever going to be greater than a human right. Considering the scenario where Canada is in War with a nation and Government passes law to threaten the safety of Canadians of that nation-the law would be unconstitutional as it violates the human rights (Discrimination against people based on their Race, nationality or ethnic origin). Therefore, Canadians are better protected since then.

Criminal Law: Performing the task of regulating public safety, social order or morality, Criminal law includes all sensational and serious crimes like theft, murder, kidnapping, assault, and fraud. Parliament makes the laws (laws have a national scope) and violation of this law is termed as a Criminal Offence, often subjected to imprisonment as the maximum punishment.

Criminal Code of Canada, Department of Justice: Parliament pass Federal Laws (Federal Acts) to regulate situations under authority of the constitution of the Canada's national Government like security, currency, military, airports, business and industries operating across nation and internationally. Violation of Federal Law is known as Quasi-criminal Offence. Quasi-criminal offence involves fines, forced compliance, or the shutting down or seizure of businesses or property. It's rare to go to prison for breaking these kinds of laws. Provincial Governments pass Provincial Laws to regulate matters under provincial constitutional authority like property rights, natural resources, education, social services, housing, health law, and family law. Violation of Provincial Law is also known as Quasi-criminal Offence. Municipal or city governments can pass laws like bylaws to regulate matters like garbage collection or pet licenses.

Consolidated Regulations of Canada, Department of Justice: Concerned with private matters, Civil Laws regulate employment contracts, building leases, marriages, divorces, wills, and child custody agreements, and seek to protect individuals from abusing or exploiting each other, therefore governing relationships between individuals and businesses. Authority for different types of Civil Law is divided by the Constitution, between the Federal and the Provincial Governments. [5]

B. *Canadian Cyber Crime Laws*

PART 1

Art. 9 Radiocommunication Act (Illegal decoding of a satellite signal)- The exemption under section 1 is granted on the condition that if there is decoding of any encrypted subscription programming signal it shall be performed under and in accordance with an authorization from a person who has a lawful right to transmit the signal and authorize its decoding. No person shall

- knowingly send, transmit or cause to be sent or transmitted any false or fraudulent distress signal, message, call or radiogram of any kind;
- without lawful excuse, interfere with or obstruct any radiocommunication;
- decode an encrypted subscription programming signal or encrypted network feed otherwise than

under and in accordance with an authorization from the lawful distributor of the signal or feed;

- operate a radio apparatus so as to receive an encrypted subscription programming signal or encrypted network feed that has been decoded in contravention of paragraph (c); or
- retransmit to the public an encrypted subscription programming signal or encrypted network feed that has been decoded in contravention of paragraph (c).

Every person who contravenes subsection 9(1.1) or (2) is guilty of an offence punishable on summary conviction and liable

- in the case of an individual, to a fine not exceeding twenty-five thousand dollars or to imprisonment for a term not exceeding one year, or to both; and
- in the case of a person other than an individual, to a fine not exceeding seventy-five thousand dollars.

Art. 10 Radiocommunication Act (Possession, sale, installation, etc. of material or device that enables the illegal decoding of a satellite signal)

(1) Every person who

- contravenes section 4 or paragraph 9(1)(a) or (b),
- without lawful excuse, manufactures, imports, distributes, leases, offers for sale, sells, installs, modifies, operates or possesses any equipment or device, or any component thereof, under circumstances that give rise to a reasonable inference that the equipment, device or component has been used, or is or was intended to be used, for the purpose of contravening section 9,
- contravenes or fails to comply with an order issued by the Minister under paragraph 5(1)(l),
- contravenes subsection 5(1.5), or

contravenes or fails to comply with a regulation, where no punishment is prescribed by regulations made under paragraph 6(1)(r) for that contravention or failure to comply,

is guilty of an offence punishable on summary conviction and is liable, in the case of an individual, to a fine not exceeding five thousand dollars or to imprisonment for a term not exceeding one year, or to both, or, in the case of a corporation, to a fine not exceeding twenty-five thousand dollars.

(2) Every person is guilty of an offence punishable on summary conviction and is liable to a fine not exceeding five thousand dollars, who

- contravenes or fails to comply with subsection 8(5) or (6) or 8.1(4); or
- does not submit the information required by the inspector under subsection 8(5.1).

Art. 42 Copyright Act (Offences related to copyrighted property)- It is an infringement of copyright for any person to do, without the consent of the owner of the copyright, anything that by this Act only the owner of the copyright has the right to do.
Every person who commits an offence under following subsection

- on conviction on indictment, to a fine of not more than $1,000,000 or to imprisonment for a term of not more than five years or to both; or
- on summary conviction, to a fine of not more than $25,000 or to imprisonment for a term of not more than six months or to both.

PART 2 Offences against Public Order
Art. 83.223 Participating, Facilitating, Instructing and Harboring- If a judge is satisfied by information that there is some material that is terrorist propaganda or computer data that makes terrorist propaganda available, the judge may order the custodian to-

- Present an e-copy of the material to the court.
- Material is no longer stored on and made available through the computer system.

PART 5 Sexual Offences, Public Morals and Disorderly Conduct
Art. 162 Publication of an intimate image without consent- Anyone publishing, circulating, transmitting, selling intimate image of a person without his/her consent is guilty of-

- an indictable offence and liable to imprisonment for a term of not more than five years
- of an offence punishable on summary conviction

Art. 163.1 Offence Tending to corrupt Moral (Obscene Materials)- Every person commits an offence who makes, prints, publishes, distributes, circulates or has in possession any obscene written matter, picture, model, phonography record or any other obscene thing.

Obscene matter refers to-

Child pornography- Any photo, depiction, video or audio recording which includes a person under the age of 18 involving in an explicit sexual activity.

Making Child pornography- Every person commits an offence who makes, publishes, or possess child pornography is guilty of indictable offence and liable to imprisonment of not more than 14 years and minimum of 1 year.

Distribution of Child pornography- Every person commits an offence who makes available, sells, distributes, advertise, imports, exports or possesses child pornography is guilty of indictable offence and liable to imprisonment of not more than 14 years and minimum of 1 year.

Possession of Child pornography-Every person who possess any child pornography is guilty of –

- Indictable offence and liable to imprisonment of not more than 10 years and minimum term of 1 year.
- Summary conviction and imprisonment of not more than two years less a day and minimum of six months.

Accessing Child pornography- Every person who accesses any child pornography is guilty of-

- Indictable offence and liable to imprisonment of not more than 10 years and minimum term of 1 year.
- Summary conviction and imprisonment of not more than two years less a day and minimum of six months.

Art. 172.1 Luring a Child- Every person commits an offence who by means of telecommunication, communicates with a person who is below 18 for the facilitation of certain laws and lures him/her to something illegal.

Punishment-

- Guilty of indictable offence of imprisonment of not more than 14 years and minimum of one year.
- Guilty of summary conviction and imprisonment of not more than two years less a day and minimum of six months.

Art. 172.2 Disorderly Conduct (Agreement or arrangement-sexual offence against child)- Every person Commits an offence who, by means of telecommunication, agrees with a person or arranges with a person to commit an offence.

Punishment-

- Guilty to an indictable offence and liable to imprisonment of not more than 14 years and minimum of 1 year.
- Guilty of summary conviction and imprisonment of not more than two years less a day and minimum of six months.

PART 6 Invasion of Privacy

Art. 184 Interception of Communications-

(1) Everyone who, by means of any electro-magnetic, acoustic, mechanical or other device, willfully intercepts a private communication is guilty of an indictable offence and liable to imprisonment for a term not exceeding five years.

Saving provision

(2) Subsection (1) does not apply to

- a person who has the consent to intercept, express or implied, of the originator of the private communication or of the person intended by the originator thereof to receive it;
- a person who intercepts a private communication in accordance with an authorization or pursuant to section 184.4 or any person who in good faith aids in any way another person who the aiding person believes on reasonable grounds is acting with an authorization or pursuant to section 184.4;
- a person engaged in providing a telephone, telegraph or other communication service to the public who intercepts a private communication,

  (i) if the interception is necessary for the purpose of providing the service,

  (ii) in the course of service observing or random monitoring necessary for the purpose of mechanical or service quality control checks, or

  (iii) if the interception is necessary to protect the person's rights or property directly related to providing the service;
- an officer or servant of Her Majesty in right of Canada who engages in radio frequency spectrum management, in respect of a private communication intercepted by that officer or servant for the purpose of identifying, isolating or preventing an unauthorized or interfering use of a frequency or of a transmission; or
- a person, or any person acting on their behalf, in possession or control of a computer system, as defined in subsection 342.1(2), who intercepts a private communication originating from, directed to or transmitting through that computer system, if the interception is reasonably necessary for

  (i) managing the quality of service of the computer system as it relates to performance factors such as the responsiveness and capacity of the system as well as the integrity and availability of the system and data, or

  (ii) protecting the computer system against any act that would be an offence under subsection 342.1(1) or 430(1.1).

Art.191 Possession, sale, purchase of electronic devices that permits an illegal interception of a private communication- Everyone who possess, sells or purchases any electro-magnetic, acoustic, mechanical or other device or any component thereof knowing that the design thereof renders it primarily useful for surreptitious interception of private communications is guilty of an indictable offence and liable to imprisonment for a term not more than two years.

PART 8 Offences Against the Person and Reputation

Art. 297 Defamatory Libel- A defamatory libel is a matter published, without lawful justification or excuse, that is likely to injure the reputation of any person by exposing him to hatred, contempt or ridicule or that is designed to insult the person or concerning whom it is published.

Art. 300 Punishment of libel known to be false- Everyone who publishes a libel that he knows is false is guilty of an indictable offence and liable to imprisonment for a term not exceeding 5 years.

Art. 301 Punishment for defamatory libel- Everyone who publishes a libel is guilty of an indictable offence and liable to imprisonment for a term not exceeding 2 years.

Art. 302 Extortion of libel-Everyone commits an offence who, with intent

- To extort money from any person or
- Induce a person to confer on or procure for another person an appointment or office of profit or trust.

PART 9 Offences Against Rights of Property Offences Resembling Theft

Art. 341 Fraudulent concealment- Everyone who, for a fraudulent purpose, takes, obtains, removes or conceals anything is guilty of an indictable offence and liable to imprisonment for a term not exceeding two years.

Art. 342 Theft, forgery, etc., of credit card- Every person who

- steals a credit card,
- forges or falsifies a credit card,
- possesses, uses or traffics in a credit card or a forged or falsified credit card, knowing that it was obtained, made or altered

  (i) by the commission in Canada of an offence, or

  (ii) by an act or omission anywhere that, if it had occurred in Canada, would have constituted an offence, or
- uses a credit card knowing that it has been revoked or cancelled,

is guilty of

- an indictable offence and is liable to imprisonment for a term not exceeding ten years, or
- an offence punishable on summary conviction.

Art. 342.01 Instruments for copying credit card data or forging or falsifying credit cards- Every person is guilty of an indictable offence and liable to imprisonment for a term of not more than 10 years, or is guilty of an offence punishable on summary conviction, who, without lawful justification or excuse, makes, repairs, buys, sells, exports from Canada, imports into Canada or possesses any instrument, device, apparatus, material or thing that they know has been used or know is adapted or intended for use

- in the copying of credit card data for use in the commission of an offence under subsection 342(3); or
- in the forging or falsifying of credit cards.

Art. 342.1 Unauthorized use of computer- This law states anyone using computers for illegal, fraudulent or criminal activities is liable for a sentence for a term of not more than 10 years. Use means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted any unauthorized function of computer.

Art. 342.2 Possession of device to obtain computer service- Everyone who uses computer service as hacking tools.
Punishment:

- Guilty of an indictable offence and liable to imprisonment for a term of not more than two years
- Guilty of an offence punishable on summary conviction.

Art. 354 Possessing of Data, Password, lists, etc. criminally obtained-Everyone commits an offence who has in possession any data, password, lists etc. obtained illegally is-

- Guilty of indictable crime and is liable of imprisonment of a term not exceeding two years
- Guilty of an offence punishable by summary conviction

PART 10 Fraudulent Transactions Relating to Contracts and Trade

Art. 380 Frauds- Everyone who, by deceit, falsehood or other fraudulent means, whether or not it is a false presence within the meaning of this Act, defrauds the public or any person, whether ascertained or not, of any property, money or valuable security or any service is

- Guilty of an indictable offence and liable to a term of imprisonment not exceeding fourteen years, where the subject-matter of the offence is a testamentary instrument or the value of the subject-matter of the offence exceeds five thousand dollars
- Guilty of indictable crime and is liable of imprisonment of a term not exceeding two years
- Guilty of an offence punishable by summary conviction

Art. 406 Forging Trademark- Everyone forges a trademark, who

- Without the consent of the proprietor of the trademark, makes or reproduces in any manner that trademark or a mark so nearly resembling it as to be calculated to deceive or,
- Falsifies, in any manner, a genuine trademark.

Punishment-

Everyone who commits an offence regarding forging or trademark is guilty of-

- Guilty of indictable crime and is liable of imprisonment of a term not exceeding two years
- Guilty of an offence punishable by summary conviction

PART 11 Willful and forbidden acts in respect of certain property

Art. 430. Mischief- Mischief in cybercrime implies- Destroying or altering computer data, Tampering or rendering Computer data, meaningless Lawless use of Computer data, Obstructing, interrupting or interfering with a person in the lawful use of computer data.

Punishment-

- The performer is guilty of indictable offence and liable to imprisonment for a term not exceeding 10 years.
- Guilty of an offence punishable on summary conviction.

Art. 432 Unauthorized recording of a movie- A person, who without the permission of theatre manager records a performance of a cinematographic work within the meaning of section 2 of the Copyright Active or its soundtrack is

- Guilty of indictable crime and is liable of imprisonment of a term not exceeding two years
- Guilty of an offence punishable by summary conviction

Unauthorized recording for the purpose of sale- A person, who without the permission of theatre manager records a performance of a cinematographic work within the meaning of section 2 of the Copyright Active or its soundtrack for the purpose of sale, rental or other commercial distribution of a copy of the cinematic work is

- Guilty of indictable crime and is liable of imprisonment of a term not exceeding five years
- Guilty of an offence punishable by summary conviction

PART 15 Special Procedure and Powers

General Powers of Certain Officials

Art. 487 Video surveillance- A warrant issued under subsection (1) that authorizes a peace officer to observe, by means of a television camera or other similar electronic device, any person who is engaged in activity in circumstances in which the person has a reasonable expectation of privacy shall contain such terms and conditions as the judge considers advisable to ensure that the privacy of the person or of any other person is respected as much as possible. [7]

C. *Organizations against Cybercrime in Canada*

Government of Canada being the most valuable tool for Canadian people, business and the government; swears to combat cybercrime threats. With increase in technology and cyber space, threats to our cyber security and quality of life has also increased. Any sort of criminal offence where computer is either object or used as a tool to perform material component offence. Cyber criminals use computer, optical or digital system for storage and communication. Various departments of the government work towards protection of Canadian citizens from cybercrime threats. There are international, provincial and federal law enforcement partnerships that have been established to combat internet and mass-marketing fraud. Examples of such coordination are as follows:

Royal Canadian Mounted Police (RCMP): RCMP being the national police service of Canada, is also a federal, provincial and municipal policing body. RCMP's aim is to prevent and investigate crime, maintain peace and enforce laws, provide security to the nation by ensuring safety of state officials, visiting foreign missions, support vital operations within Canada and abroad. It exists service to 3 territories and 8 provinces except Ontario and Quebec. It is multifaceted and an agency of Ministry of Public Safety of Canada, as outlined in section 18 of RCMP act. Canada's cyber Security Strategy was launched by the government in 2010 in order to ensure protection of Government, business and critical infrastructure of the people from Cybercrimes. [6] [7]

Technical Investigation Services (TIS): RCMP's TIS is team that provides technical domain expertise and digital forensic services to all level policing of cybercrime investigations in the country. TIS is a team that provides specialized services related to cybercrime in Canada [9].

Integrated Technological Crime Units (ITCU): RCMP's ITCU collaborates with other police departments to respond to incidents of cybercrime in the national and international scope. They process and analyze digital evidence involving cyber forensics, network system analysis, data recovery and retrieval, malware, reverse engineering, and acquiring operational tools to support cybercrime investigative techniques [9].

National Child Exploitation Coordination Centre (NCECC): The RCMP NCECC combats online sexual exploitation of children by working with the government and non-government agencies, industry stakeholders across Canada as well as internationally and law enforcement partners [9].

Canadian anti-fraud Centre (CAFC): It is the central repository of Canada for data and resource material to collect criminal intelligence and relevant information regarding matters such as mass marketing fraud, internet fraud and identification theft complaints. It provides accurate, timely and most useful information to help Canadian as well as Global citizens, business, law enforcements and government. Primary goal is to prevent disruption of criminal activities through education and awareness, dissemination of intelligence, support law enforcement and maintain economic

integrity of Canada by strengthening partnership between private and public sectors [9].

Canada's Anti-Spam Legislation (CASL): Being created in 2014 to combat spam and enforce effective email marketing, CASL also provides support regarding issues like identity theft, phishing and spread of malicious software such as virus, worms and malware [9].

Sûreté du Quebec (SQ): Being the provincial police force for the Canadian province of Quebec, SQ is the second largest provincial force and fourth largest force in Canada. No official English name exists for SQ and it is also known as Quebec Provincial Police [9].

Computer Emergency Response Team (CERT): Also known as Computer Emergency Readiness Team or Computer Security Incident Response Team (CSIRT), CERT is an expert team taking care of cyber security incidents. Due to existence of malware like computer worms or viruses that caused an incident at IBM VNET where Morris worm hit the internet on November 1988, CERT was created under US government contract at Carnegie Mellon University [9].

Ontario Provincial Police (OPP): Being one of the North America's largest police service, OPP is the division of Ministry of Solicitor General present in every community across Ontario. OPP provides necessary services to ensure safety and security of people of the Province Ontario. It is largest police service in Ontario and second largest on Canada [9].

Competition Bureau of Canada: Being an independent law enforcement agency, Competition Bureau support business and consumer prosperity in a competitive and innovative marketplace. It is headed by Commissioner of Competition and is responsible for administration and enforcement of Competition Act, Textile Labelling Act and Precious Metals Marking Act. It is a federal body office that takes care of Canada's science, innovation and economic development. Federal Government also enforced Canada's cyber security strategy, Canada's anti-spam Legislation (CASL), Canadian Radio television and Telecommunications commission (CRTC) etc. [9].

Department of Justice: DOJ is a department of Government of Canada representing Canadian Government in legal matters and it also supports both Minister of Justice and Attorney General of Canada. It works to ensure that federal government is provided with high quality legal services thereby maintaining fair, relevant, accessible and reflective of Canadian values. Along with developing policies to draft and reform laws to help federal government as and when needed, DOJ also acts as government's legal adviser to provide legal counsel and support, representing Canadian Government in the court etc [9].

Public Safety of Canada: It ensures coordination between all agencies and departments of the federal government which take care of national security and safety Canadian citizens. It protects Canadians from natural disasters, crime, terrorism and other risks. Along with building a safe and resilient Canada, it aims to achieve safe and secure Canada and powerful communities through excellent leadership. It coordinates an integrated approach to emergency management, law enforcement corrections, crime prevention and border security. It works with 5 agencies and 3 review bodies, united to form a single portfolio and all headed by Minister of Public Safety. Minister of Border Security and Organized crime reduction coordinates to reduce gang violence and tackled organized crime [9].

Global Affairs Canada: It manages Canada's diplomatic relations by providing consular services to Canadians and promoting country's international trade and leads Canada's international development and humanitarian assistance [9].

Canadian Security Intelligence Service (CSIS): Being Canada's primary national intelligence service, CSIS collects, analyses, reports and spreads intelligence on threats to the country's national security. Along with conducting operations, covert and overt inside and outside Canada, CSIS also reports to and advises the Government of Canada on country's security issues. CSIS being responsible to parliament through Minister of Public Safety, it is also to overseen by Federal Court and National Security and Intelligence Review Agency. [9]

D. *Cyber Crime Tools in Canada*

International Tools:

Convention on Cybercrime and additional Tools (November 2001): The Convention on Cybercrime or the Budapest Convention on Cybercrime or the Budapest Convention, being the first international treaty seeking to address Internet & computer crime (cybercrime) by integrating national laws, improving investigative techniques, and increasing cooperation among nations. [1][2] The explanatory report was adopted at 109th session on 8 November 2001. As of March 2019, 63 states ratified it with 4 states signing but yet to ratify it. Canada is a powerful supporter of council of Europe Convention on Cybercrime. Also known as Budapest Convention, it is not only a binding international tool designed to combat cybercrime in specific but also develops comprehensive national legislation against cybercrime and promotes international cooperation between State Parties.

United Nations Convention against Transnational Organized Crime (May 2002): The United Nations Convention against Transnational Organized Crime, adopted by General Assembly resolution 55/25 of 15 November 2000, is the international instrument in the fight against transnational

organized crime. At a high-level political conference held in Palermo, Italy, on 12-15 December 2000, it closed for approval by Member States and joined into effect on 29 September 2003. It comprises of three Protocols targeting particular regions and manifestations of organized felony: The Protocol on Preventing, Suppressing and Punishing Trafficking in Persons, Women and Children in particular; Protocol against land, sea and air smuggling of migrants and Protocol against the illicit manufacture and trafficking of firearms, their components and ammunition. This reflects a significant leap forward in combating transnational organized activity and recognizing the severity of the issues presented by Member States, as well as the need to promote and improve near global collaboration to address these issues. States ratifying this undertake to take a sequence of steps against transnational organized crime, including the establishment of national criminal crimes (involvement in an organized criminal group, money laundering, bribery and judicial interference) ; Adopting fresh and comprehensive frameworks for extradition, shared legal aid and collaboration in the field of law compliance ; and promoting instruction and technical aid to build or upgrade the required ability of domestic officials.

G-8 Moscow (October 1998) and Mont-Tremblant (May 2002) discussions: The Eight Group (G8) is an association of extremely developed nations that has established a place for the industrialized world as rulers and pacesetters. The Group of Eight (G8) is eight of the economically major nations in the world that gather regularly to tackle global financial problems in a cooperative attempt. The group's roots trace back to 1975, when it was then called the G6, with accession composed of the United Kingdom, the United States, France, West Germany, Italy, and Japan. Canada's inclusion presently constitutes the G8 cohort.

Legal aid and extradition treaties (USA, France, England, etc.): Extradition in Canada is conducted in conformity with the Extradition Act, international treaties and the Charter of Rights and Freedoms. All individuals are afforded fair treatment and due process.

Extradition from Canada: Request for extradition

- Canada may, at the request of a foreign state or entity which is an extradition partner under the Canada Extradition Act, extradite persons to stand trial, impose a sentence or serve a sentence.
- An individual may be extradited from Canada only if both nations recognize the supposed criminal behavior in issue and for which extradition is asked. Since communications between states are privileged, all information relating to specific cases is confidential and cannot be published openly until an extradition warrant is issued for detention. Following this phase, on a case-by-case basis, government data may be published. However, even if a situation is ongoing in the judiciary, if the tribunal grants a publication ban, the data may remain secret.
- The overseas nation may pursue the extradition of a individual in two respects: by submitting an official application for extradition and promoting paperwork to Canada or by requiring the temporary detention of the individual to be accompanied by an official petition for extradition.

There are three phases to the extradition process: (1) Authority to proceed: the choice to start the trials by granting an Authority to proceed ; this choice is taken by representatives of the Department of Justice. (2) Judicial phase: extradition trial before a supreme judicial magistrate . (3) Ministerial Phase: the decision on surrendering, which must be made by the Minister of Justice. This decision cannot be delegated to officials. [8]

Canadian National Tools:

Canadian Charter of Right: The Canadian Charter of Rights and Freedoms protects several rights and freedoms, including freedom of expression and the right to equality. It is the largest law in Canada as portion of our Constitution and one of the biggest achievements of our country. The Charter of Rights and Freedoms (the Charter) preserves fundamental liberties and liberties that are crucial to maintaining a safe and democratic community in Canada. It guarantees that the state or anyone operating on its behalf does not remove these rights or liberties or interfere with them. With the authority to impact our community by translating legislation and practices, it is a strong force for advancement, security, empathy and justice.

Mutual Legal Assistance in Criminal Matters Act: It's an agreement among 2 or more nations that come together to gather and exchange data to enforce public or criminal laws. There is a mechanism that has been developed among such nations to request and get access to data concerning evidence for investigation and prosecution of criminals. Evidence, legal assistance like witness statements or service documents, when needed from a foreign country, nations may cooperate informally through police agencies and request for mutual legal assistance like examining or identifying people, place and things, custodial transfer and providing help with movement of tools of criminal activity. Assistance may be denied due to political or security reasons of the nation or if criminal offence is not equally punishable in both nations. It has a structure as follows.

PART I -Foreign Investigations or Other Proceedings in Respect of Offences: It has sections like International Criminal Court, Foreign Orders for Restraint, Seizure and Forfeiture of Property in Canada, Search and Seizure, Production Orders, Arrest Warrant, Examination of Place or Site, Transfer of Detained Persons, Lending Exhibits and Appeal.

PART II - Admissibility in Canada of Evidence Obtained Abroad Pursuant to an Agreement

PART III - Implementation of Agreements in Canada: It has sections like Special Authorization to Come Into Canada, Detention in Canada, Determination of the Validity of Refusals and Privilege for Foreign Records.

PART IV - Consequential Amendments and Coming into Force
It has sections like Criminal Code, Crown Liability Act, Immigration Act and Coming into Force.

Criminal Code of Canada (C.C.C.): An Act respecting the Criminal Law. Act includes

(a) an Act of Parliament,

(b) an Act of the legislature of the former Province of Canada,

(c) an Act of the legislature of a province, and

(d) an Act or ordinance of the legislature of a province, territory or place in force at the time that province, territory or place became a province of Canada; (loi)

Income Tax Act: Tax payable by persons resident in Canada

(1) An income tax shall be paid, as required by this Act, on the taxable income for each taxation year of every person resident in Canada at any time in the year.

Taxable income:
(2) The taxable income of a taxpayer for a taxation year is the taxpayer's income for the year plus the additions and minus the deductions permitted by Division C.

Tax payable by non-resident persons:
(3) Where a person who is not taxable under subsection 2(1) for a taxation year

(a) was employed in Canada,

(b) carried on a business in Canada, or

(c) disposed of a taxable Canadian property,

Excise Act: This enactment introduces a modern framework for the taxation of spirits, wine and tobacco. It re-enacts existing provisions in the Excise Act and the Excise Tax Act relating to the excise levies on these products, together with technical improvements, and incorporates a range of new provisions. The key features of the enactment include the following:

(a) the continued imposition of a production levy on spirits, tobacco products and raw leaf tobacco and the replacement of the existing excise levy on sales of wine with a production levy at an equivalent rate;

(b) the replacement of the excise duty and excise tax on tobacco products other than cigars with a single excise duty;

(c) the introduction of excise warehouses to allow for the deferral of the payment of the production levy on domestic and imported spirits and wine to the time of sale to the retailer;

(d) more comprehensive licensing requirements and new registration requirements for persons carrying on activities in relation to goods subject to duty;

(e) explicit recognition of limited exemptions for certain goods produced by individuals for their personal use;

(f) tight new controls on the possession and distribution of goods on which duty has not been paid;

(g) modern provisions concerning the use of spirits and wine for non-beverage purposes and the use of specially denatured alcohol;

(h) updated administrative provisions, including new remittance, assessment and appeal provisions that are similar to those under the Goods and Services Tax/Harmonized Sales Tax legislation;

(i) updated enforcement provisions, including new offence, penalty and collection provisions; and

(j) transitional provisions applicable to spirits, wine and tobacco products produced before the enactment comes into force.

Customs Act: The owner or operator of

(a) any international bridge or tunnel, for the use of which a toll or other charge is payable,

(b) any railway operating internationally, or

(c) any airport, wharf or dock that receives conveyances operating internationally and in respect of which a customs office has been designated under section 5

shall provide, equip and maintain free of charge to Her Majesty at or near the bridge, tunnel, railway, airport, wharf or dock adequate buildings, accommodation or other facilities for the proper detention and examination of imported goods or for the proper search of persons by customs officers. [8]

ECUADOR

Ecuador is a country located in the northwestern region of the South American continent. This country is governed as a rule of law that functions under the principles of fundamental rights and social justice. It also defines itself as a sovereign, unitary, intercultural and plurinational country. Its official language is Spanish, and it is spoken as a first language by 93% of the populations. In addition, there are other indigenous languages, such as Quechua and Shuar, which are not considered official languages but are widely spoken around the country, specially the Quechua.

In 2008, following a popular consultation process proposed by the Ecuadorian government, the citizens democratically decided to restructure the country's social, legal and political system. One of the measures taken was the implementation of a new Constitution, which is considered the highest legal norm within the Ecuadorian legal system.

A. *Legal and Judicial System in Ecuador*

Judicial System in Ecuador

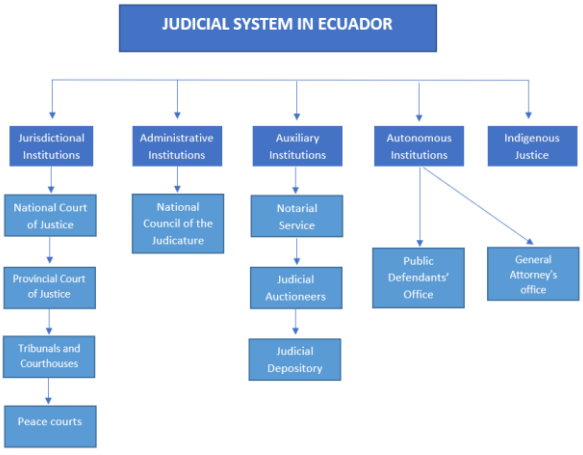


Figure 2. Judicial System in Ecuador

Among the country's main judicial institutions are:

- National Court of Justice: Represents the highest court, as well as the highest jurisdictional instance of the Judicial Branch in Ecuador. It has jurisdiction over the entire national territory. It is made up of 21 judges who hold office for 9-year terms and cannot be re-elected.
- Provincial Courts of Justice: Each of Ecuador's 21 provinces has a Provincial Court of Justice, which has jurisdiction over its territory. Judges will be organized in specialized chambers in matters corresponding to those of the National Court of Justice. These courts are responsible for imparting the law at the provincial level in accordance with the principles of the National Court of Justice.
- National Council of the Judicature: This is not a jurisdictional institution and is not among its tasks to administer justice like the National Court of Justice or the Provincial Courts of Justice. Its functions are the administration and maintenance of the country's other Judicial Branch institutions. In addition, they are responsible for evaluating judges and public officials of the Judicial Branch and imposing sanctions for misconduct if necessary.
- Public Defendants' Office: This is an autonomous institution of the Judiciary. Its objective is to guarantee access to justice to all persons who cannot contract legal defence services for the protection of their rights, whether for economic, social or cultural reasons.
- Attorney General's Office: It is an independent body in charge of directing the judicial processes in criminal matters in the country. [11]

Legal System in Ecuador

The main source of law in many countries, are the laws. These are written by codes and statutes defined by the legal bodies of each country.

The Legal System used in Ecuador is the Common Law system. In this system, judges have to decide the sentence of a trial, based on what is written in the law. Most of their work focuses on the interpretation of laws for the application of justice. In other words, in the Civil Law System, the laws established by each country are the basis for the decisions of the judges in each legal case.

Types of Law in Ecuador

In Ecuador, the National Assembly is the organism in charge of the approval of laws, resolutions and agreements, referring to diverse subjects that involve the national interest. Fundamentally, there are two types of laws that are contemplated in the Ecuadorian state. These are:

- Organic law: This type of law focuses on the regulation of the organization and functioning of the institutions created by the Constitution. In addition, the regulation of the exercise of constitutional rights and their guarantees.

Also, the regulation of the organization, competences, faculties and functioning of the decentralized autonomous governments. And finally, laws related to the political party system and the electoral system.

- Ordinary law: All the laws that are not defined by the previous section can be considered as Ordinary laws. In Ecuador, Organic Laws have a higher hierarchy than Ordinary Laws. [10]

One of the main differences between these two types of laws lies in the number of votes required from the National Assembly members for the approval of the law in question. In the case of Ordinary Laws, an absolute majority is required, which is the half of the members plus one. Whereas for Organic Laws a majority of 75% of the National Assembly members is required.

Hierarchy in Ecuadorian laws

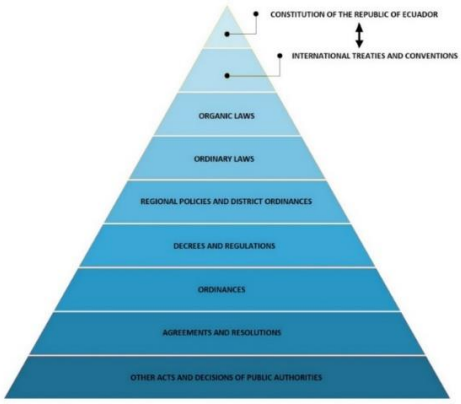


Figure 3. Hierarchy of laws in Ecuador

B. *Ecuadorian Cybercrime Laws*

Cybercrime in Ecuador is a relatively new topic. It was not until 2014 that certain laws related to computer crimes were incorporated into the Penal Code (COIP) of Ecuador to regulate this type of criminal activity.

Codigo Organico Integral Penal

SECTION FOUR (Crimes against sexual and reproductive integrity)

Article. 103.- Pornography using children or adolescents - Any person who photographs, films, records, produces, transmits or edits visual, audiovisual, computer, electronic or any other physical medium or format that contains the visual representation of real or simulated nudity or half-nudity of children or adolescents in a sexual attitude shall be punished with imprisonment from thirteen to sixteen years.

If the victim, in addition, suffers some type of disability or serious or incurable illness, it will be sanctioned with a custodial sentence of sixteen to nineteen years.

When the offender is the father, mother, relative up to the fourth degree of consanguinity or second degree of affinity, guardian, legal representative, curator or belongs to the intimate environment of the family; minister of worship, teacher, teacher, or person who by his profession or activity has abused the victim, shall be punished with imprisonment from twenty-two to twenty-six years.

Article. 173.- Sexual contact with minors under the age of eighteen by electronic means - Any person who, by electronic or telematic means, proposes to arrange a meeting with a person under the age of eighteen, provided that such proposal is accompanied by material acts aimed at rapprochement for sexual or erotic purposes, shall be subject to a prison sentence of one to three years.

When the rapprochement is obtained by coercion or intimidation, it shall be punishable by a term of imprisonment of three to five years.

A person who, by impersonating a third party or by using a false identity by electronic or telematic means, establishes communications of sexual or erotic content with a person under the age of eighteen or with a disability, shall be sentenced to three to five years' imprisonment.

The person who uses or facilitates electronic mail, chat, instant messaging, social networks, blogs, photoblogs, network games or any other electronic or telematic means to offer sexual services with minors under eighteen years of age shall be punished with a prison sentence of seven to ten years.

Article. 174.- Offering sexual services to children under the age of eighteen by electronic means - Any person who uses or provides e-mail, chat, instant messaging, social networks, blogs, photoblogs, network games or any other electronic or telematic means to offer sexual services to minors under the age of eighteen shall be liable to a term of imprisonment of between seven and ten years.

SIXTH SECTION (Crimes against the right to personal and family privacy)

Article 178. - Violation of privacy - Any person who, without the consent or legal authorization, accesses, intercepts, examines, retains, records, reproduces, disseminates or publishes personal data, data messages, voice, audio and video, postal objects, information contained in computer media, private or confidential communications of another person by any means, shall be liable to a term of imprisonment of one to three years.

SECTION NINE (Crimes against the right to property)

Article. 186. - **Fraud** - A person who, in order to obtain a pecuniary benefit for himself or for a third person by simulating false facts or by deforming or concealing true facts, misleads another person in order to perform an act that damages his or a third person's patrimony shall be liable to a term of imprisonment of five to seven years.

The maximum penalty shall apply to the person who:

1. Fraud by using a credit, debit, payment or similar card, when it is altered, cloned, duplicated, stolen, stolen or obtained without the legitimate consent of its owner.
2. Fraud through the use of electronic devices that alter, modify, clone, or duplicate the original devices of an ATM to capture, store, copy, or reproduce credit, debit, payment, or similar card information.
3. Give false certification about the operations or investments made by the legal entity.
4. Induces the public purchase or sale of securities by means of any deceptive or fraudulent act, practice, mechanism or contrivance.
5. Make quotes or fictitious transactions about any security. A person who harms more than two persons or the amount of their harm is equal to or greater than fifty unified basic wages of the worker in general shall be punished with imprisonment of seven to ten years.

Fraud committed through an institution of the National Financial System, of the popular and solidarity economy that carries out financial intermediation through the use of private public funds or Social Security, will be sanctioned with a custodial sentence of seven to ten years.
years.

The person who issues tickets for events in public stages or of massive concentration above the number of the capacity authorized by the competent public authority, will be punished with imprisonment from thirty to ninety days.

Note: Fourth paragraph amended by article 2 of Law No. 0, published in Registro Oficial Suplemento 598 of September 30, 2015.

Article. 190.- **Fraudulent appropriation by electronic means**: Any person who fraudulently uses a computer system or electronic and telecommunications networks to facilitate the appropriation of another's property or who seeks the non-consensual transfer of property, securities or rights to the detriment of this or a third party, for his or another person's benefit by altering, manipulating or modifying the operation of electronic networks, programs, computer systems, telematics and telecommunications terminal equipment, shall be liable to a term of imprisonment of one to three years.

The same sanction will be imposed if the infraction is committed with disablement of alarm systems or guarding, discovery or decryption of secret or encrypted keys, use of magnetic or perforated cards, use of remote opening controls or instruments, or violation of electronic, computer or other similar securities.

Article 191.- **Reprogramming or modification of information on mobile terminal equipment**: Any person who reprograms or modifies the identification information of mobile terminal equipment shall be liable to a term of imprisonment of one to three years.

Article 192.- **Exchange, marketing or purchase of information on mobile terminal equipment** - Any person who exchanges, markets or purchases databases containing identification information on mobile terminal equipment shall be liable to a term of imprisonment of one to three years.

Article. 193.- **Replacement of identification of mobile terminals**: The person who replaces the manufacturing labels of mobile terminals that contain identification information of
In the event that a person is found to be in possession of such equipment and places other labels with false or different identifying information in their place, they shall be punished by imprisonment for one to three years.

Article. 194.- **Illegal marketing of mobile terminals:** Any person who markets mobile terminals in violation of the provisions and procedures laid down in the regulations issued by the competent telecommunications **authority** shall be liable to a term of imprisonment of one to three years.

Article. 195.- **Illicit infrastructure**: Any person who possesses infrastructure, programs, equipment, databases or labels that allow the reprogramming, modification or alteration of the identification information of a mobile terminal equipment shall be subject to a custodial sentence of one to three years.

It is not a crime to open network bands for the operation of mobile terminal equipment.

THIRD SECTION (Crimes against the security of information and communication system assets)

Article 229 - **Illegal disclosure of databases** - Any person who, for his own benefit or that of a third party, discloses registered information contained in files, archives, databases or similar media, through or directed to an electronic, computer, telematic or telecommunications system; voluntarily and intentionally materializing the violation of the secrecy, intimacy and privacy of persons, shall be punished with a custodial sentence of one to three years.

If this conduct is committed by a public servant, internal bank employees or employees of institutions of the popular and solidarity economy who engage in financial intermediation or contractors, it shall be punishable by a term of imprisonment of three to five years.

Article 230 - Illegal interception of data - It shall be punishable by three to five years' imprisonment:

1. A person who, without prior judicial order, for his own benefit or that of a third party, intercepts, listens to, diverts, records or observes, in any form, a computer data at its origin, destination or within a computer system, a signal or a transmission of data or signals for the purpose of obtaining registered or available information.
2. A person who designs, develops, sells, executes, programs or sends messages, security certificates or electronic pages, links or pop-ups, or modifies the domain name resolution system of a financial or electronic payment service or other personal or trusted site in a way that induces a person to enter an address or Internet site other than the one he or she wants to access.
3. The person who through any means copies, clones or commercializes information contained in magnetic strips, chips or other electronic device that is supported on credit, debit, payment or similar cards.
4. The person who produces, manufactures, distributes, possesses or provides materials, electronic devices or computer systems intended for the commission of the crime described in the preceding paragraph.

Article. 231.- Electronic transfer of patrimonial assets - A person who, with a profit motive, alters, manipulates or modifies the operation of computer or telematic software or system or data message, in order to obtain the non-consented transfer or appropriation of a patrimonial asset of another person to the detriment of this or a third party, shall be sanctioned with a prison sentence of three to five years.

The same penalty shall apply to any person who provides or provides information on his bank account with the intention of illegitimately obtaining, receiving or capturing an asset through an electronic transfer of the proceeds of this offence for himself or for another person.

Article. 232.- Attack on the integrity of computer systems: A person who destroys, damages, erases, deteriorate, alter, suspend, block, cause malfunction, unwanted behavior or delete computer data, electronic mail messages, information processing systems, telematics or telecommunications to all or parts of its governing software components, shall be punishable by a term of imprisonment of three to five years.

The same penalty shall be imposed on any person who:

1. Designs, develops, programs, acquires, sends, introduces, executes, sells or distributes in any way, devices or malicious computer programs or programs destined to cause the effects indicated in the first paragraph of this article.
2. Destroy or alter without the authorization of its owner, the technological infrastructure necessary for the transmission, reception or processing of information in general.

If the offence is committed on computer goods intended for the provision of a public service or linked to public safety, the penalty shall be five to seven years' deprivation of liberty.

Any person who destroys or disables information classified in accordance with the Act shall be liable to a term of imprisonment of five to seven years.

The public servant or the one who, using any electronic or computer means, obtains this type of information, will be sanctioned with deprivation of liberty from three to five years.

In the case of classified information, the disclosure of which could seriously jeopardize the security of the State, the public servant in charge of the custody or legitimate use of the information which, without the corresponding authorization, reveals said information, shall be sanctioned with a custodial sentence of seven to ten years and a disqualification from exercising a public office or function for six months, provided that no other offence of a more serious nature is involved.

Article. 234.- Unauthorized access to a computer, telematic or telecommunications system: A person who, without authorization, accesses all or part of a computer system or telematic or telecommunications system, or remains within it against the will of the person who has the legitimate right to illegitimately exploit the access achieved, modify a web portal, divert or redirect data or voice traffic, or offer services that these systems provide to third parties, without paying them to legitimate service providers, shall be sanctioned with a prison sentence of three to five years. [12]

C. *Organizations against Cybercrime in Ecuador*

Cyber Defense Command of Ecuador

This organization was created on September 24, 2014 through the signing of agreement 281 by the Ministry of Defense of Ecuador. Its objective is the protection and defense of the country's critical infrastructure and strategic information.
Among its main functions is:

- "Protect the critical infrastructure of the State in the short, medium and long term."
- "Develop the capacity of Cyber Defense in: exploration, prevention, defense and response."
- "Generate a Command structure according to the Defense process management model."
- "Prepare the Cyber Defense Plan with the knowledge and analysis of the Cyber Defense Committee and the approval of the highest authority of the Ministry of Defense."
- "Coordinate with the Directorate of Cyber Defense the issues of its competence." [16]

This is a relatively new institution in the area of cybersecurity in Ecuador. Despite the Ecuadorian government's efforts to have a national cyber defense institution, it is expected that by 2021 the Cyber Defense Command will have the necessary capabilities to provide optimal computer security. [17]

National Police of Ecuador

The National Police of Ecuador is the agency responsible for "Attending to citizen security and public order and protecting the free exercise of the rights and security of persons within the national territory" [18]. This institution has a Cybercrime Investigation Unit. One of its functions is to co-operate with INTERPOL to promote the exchange of information related to cybercrime in the country.

Technological Crime Investigation Unit (Judicial Police)

The Judicial Police is the institution responsible for "carrying out technical-judicial and scientific investigation of crimes, in strict compliance with the Constitution, laws and regulations; under the direction of the Attorney General's Office; guaranteeing the resolution of cases, avoiding impunity and respecting human rights" [19]. This organization also has a Technological Crime Investigation Unit, which is responsible for acting on crimes related with the cyber world. As mentioned above, this institution is under the direction of the Attorney General's Office and cooperation between the two institutions is essential for the resolution of computer crimes.

ecuCERT

On July 18, 2014, ARCOTEL (Agency for Regulation and Control of Telecommunications) created ecuCERT, which is Ecuador's Computer Incident Response Center. This organization started from cybersecurity guidelines issued by the Organization of American States (OAS). The ecuCERT is recognized as an official national CIRT before the ITU (International Telecommunications Union).

"The purpose of ecuCERT is to establish general and specific cybersecurity criteria to guarantee the security of telecommunications services, the information transmitted and the invulnerability of the network through the joint management, with the country's telecommunications service providers, of computer security vulnerabilities and incidents. Control that these service providers adopt security measures and equipment appropriate to the needs of the user. It also carries out training activities, education and training on the proper use of technologies and cooperates internationally so that other CERTs are created". [20]

Strategic Intelligence Center (CIES)

The Strategic Intelligence Center (CIES) was created in September 2018 to replace the National Intelligence Secretariat. The CIES is responsible for "exercising stewardship of the National Intelligence System and producing strategic intelligence to generate alerts and timely advice in decision-making at the highest level, contributing to Integral State Security".
In the area of cybersecurity, this organization is in charge of advising and supporting government institutions in topics such as:

- "Generation of Protocols"
- "Availability monitoring."
- "Threat monitoring."
- "Vulnerability analysis."
- "Coordination and cooperation in monitoring with international intelligence agencies." [21]

D. *International Cooperation*

Treaties related to Cybercrime

Despite the fact that cybercrime is typified in Ecuador's COIP, when it comes to incidents originated in other countries, it is important to cooperate with international organizations to capture and prosecute criminals. Unfortunately, Ecuador still needs to develop alliances and join certain relevant initiatives in the area of cybersecurity in order to guarantee protection against possible computer threats to State assets and their citizens.

The Budapest Convention on Cybercrime is one of the most relevant international initiatives this treaty seeks cooperation between countries in order to combat cybercrime from a global perspective. Unfortunately, Ecuador is not yet a party to this agreement, but it is hoped that in the coming years it will be able to become a party of it.
In any case, there are other agreements directly or indirectly related to the cyber-crime to which Ecuador is subscribed, some of these are:

- The Berne Convention on Copyright.
- The Convention for the Protection and Production of Phonograms in 1971.
- The Paris Convention, which established copyright with respect to industrial property (patents, trademarks, etc.) in 1999.
- International Telecommunication Convention signed in Kenya in 1982. [13]

Alliances to fight Cybercrime

South American Defense Council (CDS)

This council, made up of 12 countries, was created by the Council of Heads of State or Government of the organization UNASUR (Union of South American Nations) in 2008. What this council seeks is cooperation and coordination in defense matters among South American countries. [26]
This council "is in charge of implementing defense policies in the areas of military cooperation, humanitarian actions and peace operations, defense industry and technology, education and training." [14]

International Telecommunication Union (ITU)

Through an agreement with the United Nations, the International Telecommunication Union implements a cybersecurity programme that offers valuable tools, critical insights, assessment and technical assistance to support particularly developing countries to increase their cybersecurity capabilities.

Forum of Incident Response and Security Teams (FIRST)

The ecuCERT (official CERT in Ecuador), a body run by the Agency for Regulation and Control of Telecommunications, has been a member of the Forum of Incident Response and Security Teams (FIRTS) since 2014. This organization is in charge of fostering coordination and cooperation in incident prevention, to stimulate fast reactions to incidents, and to encourage information sharing with members and the community at large. [15]

E. *Cybercrime Cases*

Ecuador - Case 1

Title: Hackers registered 366 fake university degrees in the informatic system of the Secretary of Higher Education, Science, Technology and Innovation (SENESCYT).

Related Law

Article. 230.- Illegal interception of data
Art. 234.- Unauthorized access to a computer, telematic or telecommunications system
Article. 370.- Illicit association

Relevant information

- The attackers violated computer systems of government and banking institutions.
- It was possible to identify these irregularities through internal audits of the SENESCYT's university degree registration system.
- There were more than 1'700,000 degrees registered in the SENESCYT system when they identified the 366 fake titles.

Case details

The Secretary of Higher Education, Science, Technology and Innovation (SENESCYT) is a government institution that, among its functions, is responsible for maintaining a register of all official university degrees. Through internal computer audits, they found that 366 university degrees registered in their system presented some "irregularities". The institution proceeded with the respective denunciation to the Attorney General's Office and then they initiated an investigation process that would last about 3 months.
In the early hours of Friday, January 8, 2016, the "Impacto Inicial" operation was launched. Nine simultaneous raids were carried out in 4 provinces of Ecuador, Pichincha (Quito), Guayas (Guayaquil and Daule), Santo Domingo de los Tsáchilas and Imbabura (Ibarra). More than 100 officers of the National Police of Ecuador participated in the operation. The result was the capture of 10 suspects. Among the evidence confiscated were: cell phones, laptops and desktops, pen drives, hard drives, hundreds of bank deposits,

credentials, supposedly false letterheads, Ministry of Education seals, etc.
Interior Minister José Serrano in a press conference gave the following details about this case:

- The alleged hacker gang would have operated for about 18 months carrying out illegal activities.
- Among the main categories of fake university titles registered in the system were: 40.6% Law, 35.9% to Commerce and Administration, 6.3% to Computer Science, 3.1% to Education Sciences and about 2% to Medicine.
- Depending on the request, the amounts that the criminals charged for registering the fake degree in SENESCYT's system ranged from USD 5,000 - 10,000. The total estimated money received by the criminals would reach USD 1'000,000.
- Most of the money received by the criminals was transferred to banks in Colombia.

Among the elements presented by the prosecutor for the formulation of charges were: follow-up and surveillance report, interception of telephone calls, technical ocular inspection report, etc. The fiscal instruction in this case will have a duration of 90 days.

Finally, the professional titles identified as fraudulent have been eliminated from the SENESCYT system, after verifying with the universities involved that there was no official information (such as academic records) of the owners of such titles. [22]

Sentence

- The names of the offenders involved in this crime have not been disclosed to the public. However, it is known that 4 of the 10 detainees have been sentenced to 24 months in prison, at the suggestion of the prosecutor, after the defendants accepted their participation in this crime. [27]

Ecuador – Case 2

Title: Use of electronic device (skimmer) to clone credit and debit cards from ATMs.

Related law

Article. 190.- Fraudulent appropriation by electronic means

Article. 230.- Illegal interception of data

Article. 370.- Illicit association

Relevant information

- Cloning of debit and credit cards using an electronic device called a skimmer.
- The criminals operated in the country for about 4 years.
- The collaboration of 4 different police agencies was needed to execute the capture of the criminals.
- The time needed to clone the credit was less than 15 minutes.

Case details

After two months of investigation by the National Police and the Anti-Crime Intelligence Unit (UIAD), it was possible to dismantle a gang of criminals who were mainly engaged in cloning debit cards, using an electronic device called skimmer, which was placed in ATMs, in different locations in the country. This criminal gang had been operating in the country since 2010 (the arrest occurs 4 years later). The "Skimmers Uno" operation is an example of a coordinated work between several local police agencies. As mentioned before, two of the institutions involved are the National Police and the UIAD, as well as the Intervention and Rescue Group (GIR), Criminalistics and 6 prosecutors of the province of Pichincha. During the operation, three buildings located in different parts of the city of Quito were raided. This operation required the collaboration of 45 agents.

Among the evidence seized in the operation was: laptops, printers, lithium batteries, micro-cameras, USB flash drives, cell phone parts, cash, dozens of credit/debit cards.
The way the gang committed the crime was as follows:

1. The first step was to know in detail where the skimmer was going to be placed. For this, the criminals took pictures of the location and especially of the ATM. Then they used these photographs in their laboratory, to build a personalized skimmer for each ATM.
2. Later they proceeded to install the skimmer in the ATM. This is a device formed by two parts. The first is a very small camera that is placed near the keyboard to capture the victim's PIN. The second component is an altered reader that copied the magnetic stripe from the victim's card. This altered reader was placed on top of the original reader.
3. Finally, the band proceeded to remove the skimmer from the ATM to avoid leaving evidence. Once the criminals had enough samples, they proceeded to print the cloned cards in their laboratories, using the information previously collected by the skimmer.

The gang of criminals consisted of 7 people. Two of them were in charge of placing and removing the ATM skimmers. In addition, there were two other people who observed the victims to verify that everything was going according to plan. Two more people worked in the laboratory, cloning and printing the cards. Finally, there was a person in charge of the group, who planned the robberies.

After the operation carried out by the National Police, the 7 members of the criminal gang were captured and

brought to trial. In theory, the penalty stipulated in Ecuador's Penal Code varies from 3 to 5 years in prison for this type of crime. However, article 635 opens the possibility the application of abbreviated procedure when offences punishable by deprivation of liberty for up to 10 years are committed**.** [23]

Sentence

- In this case, the prosecutor in charge of this case recommended to the judge on duty a 12-month prison sentence, as the offenders accepted the guilt of the crime, thus applying the abbreviated procedure described in the previous paragraph. [24]

Ecuador – Case 3

Title: Alleged suspect used fake Facebook profiles to have sex with under aged victims.

Related Law

Article. 173.- Sexual contact with minors under the age of eighteen by electronic means

Relevant information

- Creation of fake profiles on Facebook.
- Interaction with minors through social networks.
- Extortion in exchange for not disclosing the sexual material of minors.
- It was reported that sometimes the offender performed sexual acts with the victims.

Case details

On Tuesday, March 26, 2019, in the city of Baños, province of Tungurahua, a 41-year-old individual was arrested for alleged sexual crimes with minors through deception and extortion, using social networks as mean of contact with the victims. Thanks to the denunciation of several victims it was possible to identify the suspect and find his whereabouts.
The Technological Crimes Unit of the Judicial Police and the Attorney General's Office worked together in this operation, which finally ended with the arrest of the subject. At the time of his arrest, the suspect recorded six legal proceedings for different reasons in his police file.

The National Director of the Judicial Police declared in a press conference that the suspect, "hiding behind false profiles (Facebook), interacted and transmitted digital content, images in sexual acts, nudity, etc. through technological devices" with the victims. Once the perpetrator obtained the sexual content of the victims, he proceeded to extort them by threatening to disclose the sexual photos or videos in his possession. Sometimes the victim was required to have sex with the offender.

In this operation, two raids were carried out on buildings located in the center of the city. The police confiscated several electronic devices such as: cell phone equipment, tablets, SD cards, SIM cards, and a CPU for the following

After the charges have been filed, the judge on duty determines only precautionary measures against the suspect. The frustration in the prosecutor's office was evident and in an interview with the media she states that "we have had other really small cases and preventive detention has been ordered, which in this particular case did not happen". [25]

Sentence

- Suspect is released. No details of this case are given to the public, because there were under age victims involved.

IRAN

A. Legal and Judicial System in Iran

The Iranian legal system is a civil legal system, built upon a constitution, legal codes (such as the civil, commercial, criminal and procedural codes) and substantive laws. The constitution ranks highest, followed by statutes and then government decrees.
In addition, while Sharia law is not a mandatory source of law, it has a significant impact upon it as all civil, penal, financial, economic, cultural, military, political and other laws and regulations must be based on Islamic criteria [28].
The Iranian court system is divided into three tiers, all of which fall under the remit of the judiciary:

Structure of the judicial system

The 1979 Constitution of the Islamic Republic called for the judiciary to be "an independent power," and charges it with "investigating and passing judgment on grievances; Overseeing the correct implementation of legislation; uncovering offences; prosecuting, punishing and punishing criminals; adopting "appropriate steps" to avoid crime and reforming criminals [29].
The Head of the Judiciary, also recognized in English as Iran's Chief Justice, is to be a ' just Mujtahid ' designated by the Supreme Leader and serving for five-year tenure. He is accountable for establishing the organizational structure of the judiciary; writing laws for Parliament, recruiting, firing, supporting and assigning magistrates [29].

Court Structure

The composition of the Iranian court involves Revolutionary Courts, Public Courts, Peace Courts, and Cassation Supreme Courts. Revolutionary courts have 70 divisions. Public judiciary comprise of Civil, Civil Special, Criminal First Class, and Criminal Second Class. Peace judiciary are split into ordinary judiciary, and Independent Peace Courts, and Supreme Cassation Courts [29].

Operation

The Islamic Republic's judiciary are focused on an inquisitorial scheme as it occurs in France, rather than a United Kingdom's adversarial scheme. The judge decides the verdict, in serious cases, he is assisted by two secondary judges, and when involving the death penalty, four secondary judges. There is a public prosecutor, however, according to Article 168 of Iran's constitution, in certain cases involving the media, a jury is allowed to be the arbiter. The judge retains complete authority; in reality, magistrates may be overshadowed by instances, and there is no moment to excogitate about each situation. All magistrates have Islamic and Iranian law certification [29].

Court System

The judicial scheme currently comprises of overall and particular judiciary. General courts have a general jurisdiction to hear all cases except for cases within the jurisdiction of the specific courts. In most courts, in addition to the preliminary hearing, parties have the right to pleading to the court of appeal. The courts' decisions do not have any precedential value and are not usually codified or documented for future reference by other courts.

1.Dispute Settlement Councils:

Dispute Settlement Councils are part of the judiciary but are supposed to function as an alternative dispute resolution body.
Under Articles 8 and 10, sides to a conflict may undertake to file their complaint in conflict resolution commissions except in instances of marriage, divorce, will, bankruptcy, lack of capacity and property owned by the government and public [29].

2.Civil Courts:

Civil courts hear local pecuniary and nonpecuniary civil disputes that are not within the jurisdiction of Dispute Settlement Councils [29].

3.Criminal Courts

Criminal judiciary witness criminal instances and latest organizational modifications have been taking place. The latest changes in the Iranian criminal justice system are the new Islamic Criminal Code and Criminal Procedure Code passed in 2013 and 2014 respectively [29].

Criminal Procedure Act, the criminal courts are as follows:

First Class Criminal Court, Second Class Criminal Court, Revolutionary Court, Juvenile Court, and Military Court.

3.1 First Class Criminal Court:

Three magistrates are sitting in criminal courts of the First Class. Criminal courts of first class are regional. First Class Criminal Court has jurisdiction to consider the previous instances: instances of capital punishment, life sentences, amputation of limbs and bodily wounds with a third of blood money penalty, felonies of degree four and greater, political offenses and media offences. First Class Criminal Court is responsible for hearing political and media offences. Such trials must involve a jury [29].

3.2 Second Class Criminal Court:

Only one judge sits in the Second-Class Criminal Court. Second Class Criminal Courts are based in counties. The Head of Judiciary may decide to establish county courts instead of second-class criminal courts with the same jurisdiction. Second Class Criminal Court has a general jurisdiction to hear all cases except cases within the jurisdiction of special courts and First-Class Criminal Court [29].

3.3 Revolutionary Court

The revolutionary courts are in session with three judges in capital punishment, life sentence, and limb amputation, felonies on body injuries with a minimum of one-third worth of blood money punishment [29].

The revolutionary court has jurisdiction to hear all crimes against national and international security national armed terrorism insulting Imam Khomeini and the Supreme Leader, all smuggling and drugs crime [29].

Financial crimes under the jurisdiction of revolutionary judiciary are disturbance of monetary or foreign currency exchange in the nation through mass money trafficking, manufacturing or trafficking of falsified domestic or overseas coins or banknotes, triggering disturbance in the exchange of technical machinery and raw materials, attempts to smuggle cultural heritage or domestic assets are smuggling even if they are ineffective and the estate is seized by the state,

receiving a large sum of cash from actual or legal persons in the form of a collaboration and losing or disrupting the domestic economy, and conspiring to interrupt the domestic export exchange by fraud in forms of loan or sales fraud and network marketing [29].

3.4 Juvenile Court

Juvenile courts are focused in counties and the amount of divisions in each county differs. Juvenile courts have a judge and two social workers (to advise the clerk).

Juvenile courts are competent to hear instances against kids under 18 years of age. If the defendant hits 18 in the Juvenile Court trial, the proceeding will proceed. However, if the defendant hits 18 before the trial begins, the matter would be transferred to a jurisdictional criminal court. In the latter situation, the defendant will still profit from Juvenile Courts' trial privileges [29].

3.5 Military Court

Military Courts hear cases against military and police forces if the crime is related to their duties and/or happened during the hours they have been on duty [29].

4. The Supreme Court:

The Supreme Court is the highest court of appeal of both civil and criminal cases. It is based in Tehran. Each branch has three judges. The judges have to have at least 10 years of experience as a judge or a lawyer or be an Islamic scholar or have studied Islamic jurisprudence in a seminary for 10 years. The Supreme Court, as a court of appeals, does not issue a substantive decision. It only reviews cases with regards to the application and interpretation of the law. It then sends the case to the lower court to review the facts and the law for a second time and issue a new decision. Lower courts do not have to comply with the Supreme Court's decision. If the lower court issues the same decision as to its earlier decision and the defendant appeals again, the case will be referred to the Supreme Court General Council in case the Supreme Court still issues a similar judgment to its previous decision.
The Supreme Court also has jurisdiction to settle disputes between two courts from two different provinces on their jurisdiction to hear a case. It may also allow a criminal court without jurisdiction to witness a dispute if it is a more comfortable forum for sides or the location where the crime has been committed [29].
The General Council of the Supreme Court is hearing instances concerning conflicts of analysis by various lesser judiciary of civil or criminal law. The understanding of the General Council of the Supreme Court has precedent importance and can be overruled only by another judgment of the General Council of the Supreme Court or subsequent parliamentary legislation. [29]

B. Iranian Cyber Crime Laws

Iran Computer Crime Act- ICCA

Chapter 1- Crimes against Confidentiality of Data and Computer and Telecommunication Systems

Title 1- Unauthorized Access

Art. 1- Every person who, without authority, gains access to data, or computer or telecommunication systems which are protected under security measures shall be punished by a term of 91 days to 1 year of imprisonment, or by a fine of 5,000,000 to 20,000,000 Rials, or by both the imprisonment and fine.

Title 2- Unauthorized interception

Art. 2- Every person who, without authority, intercept the non-public transmissions of content by computer or telecommunication systems, or electromagnetic or optical waves shall be punished by a term of 6 months to 2 years of imprisonment, or by a fine of 10,000,000 to 40,000,000 Rials, or by both the imprisonment and fine.

Title 3- Computer Spy

Art. 3- Every person who, without authority, commits any of the following acts against stored or in transit secret data in storage media or computer or telecommunication systems shall be punished by the provided punishments:

- Gaining access to the aforesaid data or acquisition of them, or interception the content of the secret data in transit; by a term of 1 to 3 years of imprisonment, or by a fine of 20,000,000 to 60,000,000 Rials, or by both the imprisonment and fine;
- Making the aforesaid data accessible to unauthorized persons; by a term of 2 to 10 years of imprisonment;
- Disclosure of the aforesaid data or making them accessible to a foreign government, organization, corporation, or group, or their agents, by a term of 5 to 15 years of imprisonment.

Note 1: The term "secret Data" refers to the data whose disclosure will affect the state security or national interests.

Note 2: the procedure of determination and identification of the secret data, and the method of classification and protection of them shall be drafted by the Ministry of intelligence with the cooperation of ministries of Justice, State, Information and Communication Technology (ICT), and Defense, and ratified by the Board of Ministers within 3 months from the date the present act is ratified.

Art. 4- Every person who, with the intent to access the secret data provided in article 3 of the present act, violates the security measures of the computer or telecommunication

systems shall be punished by a term of 6 months to 2 years of imprisonment, or by a fine of 10,000,000 to 40,000,000 Rials, or by both the imprisonment and fine.

Art. 5- In the event that government officials who are responsible for protection of the secret data provided in article 3 of the present act or relevant systems are efficiently trained , and the mentioned data or systems have been put at their disposal -due to carelessness, negligence or nonobservance of the security measures cause the access of unauthorized persons to the mentioned data, storage media, or systems, shall be punished by a term of 91 days to 2 years of imprisonment, or by a fine of 5,000,000 to 40,000,000 Rials, or by both the imprisonment and fine, in addition to a period of 6 months to 2 years dismissal from service.

Chapter 2- Crimes against Integrity and validity of Data and Computer and Telecommunication Systems

Title 1- Computer Forgery (& counterfeiting)

Art. 6- Every person who, without authority, commits the following acts shall be considered a counterfeiter and punished by a term of 1 to 5 years of imprisonment, or by a fine of 20,000,000 to 100,000,000 Rials, or by both the imprisonment and fine:

- Alteration or creation of admissible data, or deception creation or entry of data to them;
- Alteration of data or signals stored in memory cards or processable cards in computer or telecommunication systems or chipsets, or deception creation or entry of data to them.

Art. 7- Every person who, by knowing that the data or cards or chipsets are forged, uses them shall be sentenced to the punishments provided in the above article.

Title 2- Data or Computer or Telecommunication Systems interference

Art. 8- Every person who, without authority, deletes, destroys, or disturbs another person's data available in computer or telecommunication systems or storage media, or makes them unpossessable shall be punished by a term of 6 months to 2 years of imprisonment, or by a fine of 10,000,000 to 40,000,000 Rials, or by both imprisonment and fine.

Art. 9- Every person who, without authority, disables another person's computer or telecommunication systems, or disturbs their function by inputting, transmitting, distribution, deleting, suppressing, manipulation, or deterioration of data or electromagnetic or optical waves shall be punished by a term of 6 months to 2 years of imprisonment, or by a fine of 10,000,000 to 40,000,000 Rials, or by both the imprisonment and fine.

Art. 10- Every person who, without authority, prevents authorized persons from access to data, or computer or telecommunication system by hiding data, changing passwords, and encrypting data shall be punished by a term of 91 days to 1 year of imprisonment, or by a fine of 5,000,000 to 20,000,000 Rials, or by both the imprisonment and fine.

Art. 11- Every person, with intent to endanger the public security and tranquility, commits the acts mentioned in articles (8), (9), and (10) of the present act against computer and telecommunication systems which are used to provide (vitally) needed public services, including treatment services, water, power, gas, telecommunication, transportation, and banking shall be punished by a term of 3 to 10 years of imprisonment.

Chapter 3- Computer Related Theft and Fraud

Art. 12- Every person who, without authority, thievery of data belonging to others, while the original data remains, shall be punished by a fine of 1,000,000 to 20,000,000 Rials, and otherwise, by a term of 91 days to 1 year of imprisonment, or by a fine of 5,000,000 to 20,000,000 Rials, or by both the imprisonment and fine.

Art. 13- Every person who, without authority, obtains money, property, profits, services, or financial advantages for himself or another person, by committing acts, including entering, altering, deleting, creating, suppression data, or disturbing the system shall be punished by a term of 1 to 5 years of imprisonment, or by a fine of 20,000,000 to 100,000,000 Rials, or by both the imprisonment and fine, in addition to restitution of the property.

Chapter 4- Crimes against Public Morality and Chastity [Decency]

Art. 14- Every person who produces, transmits, distributes, trades, or, with intent to transmission or distribution or trading, produces or stores pornographic contents by means of computer or telecommunication systems or storage media shall be punished by a term of 91 days to 2 years of imprisonment, or by a fine of 5,000,000 to 40,000,000 Rials, or by both the imprisonment and fine.

Note 1: Committing the aforesaid acts concerning non-pornographic but immoral contents shall result in at least one of the above punishments.

Note 2: In case the pornographic contents are sent to less than ten persons, the perpetrator shall be punished by a fine of 1,000,000 to 5,000,000 Rials.

Note 3: if the perpetrator has made the acts provided in this article his routine work or commits them in an organized way, in case that not being found guilty of corruption on the earth, shall be punished by the maximum amount of both punishments.

Note 4: "Pornographic Contents" refer to the real or unreal image, audio, or text indicating the whole nudity of a man or woman, or their sexual organs or sexual intercourse.

Art. 15- Every person who commits the following acts by means of computer or telecommunication systems or storage media shall be punished as follows:

- In case of provocation, encouraging, threatening, bribing, alluring, deceiving people to access pornographic contents, or facilitating or training the methods of gaining access to them, punished by a term of 91 days to 1 year of imprisonment, or by a fine of 5,000,000 to 20,000,000 Rials, or by both the imprisonment and fine; Committing such acts with respect to non-pornographic but immoral contents shall result in a fine of 2,000,000 to 5,000,000 Rials.
- In case of provocation, encouraging, threatening, inviting, deceiving people to commit crimes against chastity, using narcotic or psychedelic drugs, suicide, sexual deviations, or violation, or facilitating or training the means of commitment or use of them, punished by a term of 91 days to 1 year of imprisonment, or by a fine of 5,000,000 to 20,000,000 Rials, or by both the imprisonment and fine.

Note: The provisions of this article and article 14 shall not refer to the group of contents which are produced, generated, kept, represented, distributed, issued, or traded for scientific purposes or any other rational expedients.

Chapter 5- Aspersion of Dignity and Issuing Lies

Art. 16- Every person who, by means of computer or telecommunication systems, alters or distorts the video, audio, or image of another person, and issues them; or being aware of such alteration or distort, and issues them- in such a way that conventionally results in aspersion of dignity of them- shall be punished by a term of 91 days to 2 years of imprisonment, or by a fine of 5,000,000 to 40,000,000 Rials, or by both the imprisonment and fine.

Note: In the case that the mentioned alteration or distortion done is in a pornographic manner, the perpetrator shall be punished by the maximum extent of both provided punishments.

Art. 17- Every person who, by means of computer or telecommunication systems, issues or makes the audio, image, private or family video, or secrets of another person accessible to others without permission –other than in legitimate instances- in such a way that conventionally results in aspersion of the dignity of them, or causes loss- shall be punished by a term of 91 days to 2 years of imprisonment, or by a fine of 5,000,000 to 40,000,000 Rials, or by both the imprisonment and fine.

Art. 18- Every person, with intent to cause damage to another person or distress the public mind or official authorities; and by means of computer or telecommunication systems, issues or makes accessible any lies; or, with the very same intent, explicitly or implicitly, in person or by quotation attributes unreal acts to a legal or real person- whether any moral or economic loss is delivered to the committee or not- shall be punished by a term of 91 days to 2 years of imprisonment, or by a fine of 5,000,000 to 40,000,000 Rials, or by both the imprisonment and fine, in addition to reestablishing their dignity, if possible.

Chapter 6- Corporate Liability

Art. 19- In following instances, in case computer cyber-crimes are committed by the name of a legal entity and pursuant to its interests, the legal entity shall be criminally responsible [liable]:

- When computer crime is committed by the director of the legal entity;
- When the director orders the computer crime and the crime has been committed
- When any of the employees of the legal entity commits the computer crime with the director's awareness or due to the director's lack of supervision;
- When the entire activities of the legal entity or a part of them are allocated to computer crime.

Note 1: The term "Director" refers to the person who has the authority of representativeness, decision making, or supervision of the legal entity.

Note 2: The criminal liability of the legal person shall not exempt the perpetrator from punishment, and in case of lack of terms and conditions provided in the proceeding this article, or impossibility of attributing the crime to the legal entity, the sole real person shall be regarded responsible.

Art. 20- The legal entities provided in the above article, based on the circumstances of the committed crime, their income range, and the consequences of committing the crime- in addition to payment of 3 to 6 times as much as the maximum extent of fine provided for the committed crime- shall be punished as follows:

- In case the maximum punishment provided is up to 5 years, temporary closure of the legal entity from 1

to 9 months, and in the event of repeating the crime, temporary closure of the legal entity from 1 to 5 years;

- In case the maximum punishment provided is more than 5 years, temporary closure of the legal entity from 1 to 3 years, and in the event of repeating the crime, the legal entity shall be liquidated.

Note: The director of the legal entity which is liquidated based on paragraph (B) of this article shall not be allowed to found, represent, make decisions for, or supervise any other legal entity up to 3 years.

Art. 21- Access Service Providers (ISPs) are obligated to filter the criminal content which is regulated within the framework of laws, whether resulted from or used to commit computer crimes, based on the technical criteria and the list provided by the Filtering Committee subject to the following article. The ISP shall be liquidated, In case of willful refusal of filtering criminal content, and punished by a fine of 20,000,000 to 100, 000, 000 Rials, for the first time, by a fine of 100,000,000 to 1,000,000,000 Rials, for the second time, and by a three-year temporary closure, for the third time, in case of carelessly or negligently causing access to the illegal content.

Note 1: In case that the criminal content belongs to the websites of the public institutions including entities under the supervision of the Supreme Leader, and the three legislative, executive, and judiciary branches of power of the government, and the non-governmental public institutions subject to the Law of the Index of Non-governmental Public Institutions and Entities, 19/4/1373, and its amendments, or to the parties, guild or political societies, Islamic societies, recognized religious minorities, or to other legal or real persons in Iran -identification and communicating to whom is possible- the websites shall not be filtered until the issue of the final decision based on the order of judicial authority examining the case, and immediate removal of the criminal content's effect.

Note 2: Filtering the criminal content which is the subject-matter of the private plaintiff shall be carried out by the order of the judicial authority examining the case.

Art 22- The judiciary power is obligated to establish the Committee of Filtering (committee of determining the instances of criminal content), within one month from the ratification of the present act, in the location of the Office of the State Prosecutor General. The ministers or representatives of the ministries of Training and Development, Information and Communication Technology (ICT), Information, Justice, Science, Research and Technology, Culture and Islamic Guidance, the president of the Islamic Propagation Organization, and the head of the Islamic Republic of Iran Broadcasting, the Commander-in-Chief of the Police, an expert in information and communication technology chosen by the Commission of Industries and Mines of the Islamic Constative Assembly (Majlis), and one of the members of the Legal and Judicial Commission of the Islamic Constative Assembly chosen by the Legal and Judicial Commission and confirmed by the Islamic Constative Assembly, constitute the members of the committee. The State Prosecutor General shall undertake the responsibility of chairmanship of the committee.

Note 1: The committee meetings shall be held every 15 days, and the quorum shall consist of 7 members. Decisions of the committee shall be effective by a relative majority of the votes of those present at the meeting.

Note 2: The committee is obligated to examine and decide about the complaints regarding the filtered instances.

Note 3: The committee is obligated to present a report regarding the procedure of filtering the criminal content to the heads of the three powers of government
(legislative, executive, and judiciary), and the Supreme National Security Council every 6 months.

Art 23: The Hosting Service Providers are obligated to, immediately after receiving the order of the Filtering Committee mentioned in the above article or judicial authority examining the case concerning the existence of criminal content in computer systems, prevent the continuation of access to them. The Hosting Service Providers shall be liquidated, in case of willful refusal of executing the order of the committee or judicial authority. Otherwise, The Hosting Service Providers shall be punished by a fine of 20,000,000 to 100, 000, 000 Rials, for the first time, a fine of 100,000,000 to 1,000,000,000 Rials, for the second time, and by a three-year temporary closure, for the third time, in case of carelessly or negligently causing access to the criminal content.

Note: The Hosting Service Providers are obligated to, immediately after becoming aware of the existence of the criminal content, inform the Filtering Committee of their existence.

Art 24- every person who, without authority makes use of the international (internet) bandwidth to establish international protocol-based telecommunication connections from abroad to Iran or vice versa shall be punished by a term of 1 to 3 years of imprisonment, by a fine of 100,000,000 to 1,000,000,000 Rials, or by both the imprisonment and fine.

Chapter 7- Miscellaneous Crimes

Art 25- Every person who commits the following acts shall be punished by a term of 91 days to one year of imprisonment, by a fine of 5,000,000 to 20,000,000 Rials, or by both the imprisonment and fine:

- Production, issue, distribution of and making accessible, or trading data, software's, or any other

electronic devices, which are exclusively used to commit computer crimes;
- Sale, issue, distribution of, or making accessible passwords or any data makes the unauthorized access to data or computer or telecommunication systems belonging to others possible;
- Issue of or making accessible the unauthorized-access-training contents, unauthorized sniff, computer spy, causing distortion or destruction of data or computer or telecommunication systems.

Note: In the event that the perpetrator has made the mentioned acts his routine occupation, he shall be punished by the maximum extent of both punishments provided (in this article).

Chapter 8- Aggravation of Punishment

Art 26- In following instances, the perpetrator shall be punished by more than two-third of the maximum extent of one or both the punishments:

- Any of the employees or staff of the governmental or government-related departments, organizations, and institutions, councils and municipals, revolutionary entities, foundations and institutions which are administered under the supervision of the supreme leader (of the Islamic Republic of Iran), the Supreme audit court, the Institutions which are administered by means of the constant subsidies subventions paid by the government, officials holding judicial ranks, and generally, members and staff of the three powers/ branches of the government, armed forces, and public service officers -whether official or unofficial- have committed computer crimes in the performance of their duties;
- The operator or the legal possessor of the computer or telecommunications networks have committed computer crimes in the performance of their duties;
- Data or computer or telecommunication systems belong to the government or entities or centers providing public services;
- The crime has been committed on a vast scale.

Art 27- in the event of more than two times repetition of the crime, the court is empowered to deprive the perpetrator of the public electronic services including internet or cell phone subscription, obtaining domain name registrations in national Top-Level Domains (ccTLDs), and electronic banking:

- In case the imprisonment punishment provided for the crime is from 91 days to 2 years, deprivation from 1 month to 1 year;
- In case the imprisonment punishment provided for the crime be from 2 to 5 years, deprivation from 1 to 3 years;
- In case the imprisonment punishment provided for the crime be more than 5 years, deprivation from 3 to 5 years.

Section 2- Procedural law
Chapter 1- Jurisdiction

Art 28- Along with instances predicted by other Laws and regulations, The Iranian courts have jurisdiction over the following instances:

- Criminal data or data used in committing crimes have been anyhow stored in computer or telecommunication systems or data carries existing in the Islamic Republic of Iran's land, air, and maritime territory;
- The crime has been committed by means of the websites with country code Top-Level Domains of Iran;
- The crime has been committed by any Iranian or non-Iranian person, outside Iran's borders, against computer or telecommunication systems, and websites used by or under control of the three powers/ branches of the government, Leadership Entity, official governmental agents, or any institution or entity providing public services, or against websites with national country-code Top-Level Domains of Iran;
- Computer crimes involve abuse of persons under the age of 18, whether the perpetrator or the victim is Iranian or non-Iranian.

Art 29- In the event that the computer crime is discovered or reported in a place, while the location it was committed in the location of the commitment thereof is not obvious, the local prosecutor's office is obligated to initiate the preliminary investigations. In case that the location of the commitment of crime does not become obvious, the prosecutor's office- by finishing the investigations- resorts to issue a verdict, and the relevant court issues the appropriate order.

Art 30- The judiciary power is obligated to, based on necessity, allocate one or more branches of the prosecutor's office, the public and revolutionary courts, military courts, and appeal courts to try computer crimes.

Note: Judges of the aforesaid prosecution office branches and courts shall be chosen amongst judges who are well-acquainted with the computer affairs.

Art 31- In the event of any disputes arising over jurisdiction, the dispute resolution shall be done in accordance with the Civil Procedure Code of the Public and Revolutionary Courts.

Chapter 2- Collecting Digital Evidence
Title 1- preservation of traffic data

Art 32- Access service providers are obligated to preserve the traffic data at least until 6 months after the creation thereof and the users' information at least 6 months form termination of the subscription.

Note 1: The term "Traffic Data" refers to any data that computer systems generate in computer and chain of telecommunication chain make their trace from origin to destination possible. These data include information such as origin, path, date, time, duration, and volume [mass/ size] of communications and the type of the relevant services.

Note 2: The term "User Information" refers to any information related to the user of access services including the type of services, technical facilities used, duration, identity, geographical or postal address or internet protocol (IP), telephone number, and other individual characteristics of the user.

Art 33- Domestic host service providers are obligated to retain their users' information at least until 6 months, and the stored content and traffic data resulted from the occurred changes at least until 15 days from termination of the subscription.

Title 2- Expedited preservation of the Stored Computer Data

Art 34- Whenever preservation of stored computer data is necessary for doing investigations or judgments, the judicial authority is empowered to issue the preservation order addressed to any persons who, anyhow, have them under their control or possession. In urgent cases, including [such as] danger of damage, alteration, or destruction of data, judicial officers are empowered to, on their own initiative directly issue the preservation order, and then inform the judicial authority of the actions carried out within 24 hours. In the event that any of the governmental staffs, judicial officers, or other persons refuse to execute the order, disclose the preserved data, or inform the persons to whom the aforesaid data is related to the provisions of the issued order, governmental staffs and judicial officers shall be punished by refusal of executing the judicial authority's order, and other persons shall be punished by a term of 91 days to 6 months imprisonment, or by a fine of 5,000,000 to 10,000,000 Rials, or by both the imprisonment and fine.

Note 1: Data preservation is not equal to presentation or disclosure thereof, and demands necessitate observance of the relevant laws and regulations.

Note 2: the data protection duration is not to exceed 3 months, and in case of necessity, is extendable by means of the judicial authority's order.

Title 3- Data Presentation

Art 35- The judicial authority is empowered to issue the order of presentation of data mentioned in articles (32), (33), and (34) above addressed to aforesaid persons to put (the data) at the disposal of the officers. Refusal of executing the order shall be punished by the punishment provided in article (34) of the present act.

Title 4- Data and Computer and Telecommunication Systems' Search and Seizure

Art 36- Data or computer and telecommunications systems' search and seizure shall be performed by virtues of the judicial order, in cases, there is a strong suspicion concerning discovering the crime or identifying the criminal or crime evidence.

Art 37- Data or computer and telecommunications systems' search and seizure shall be performed at the presence of the legal possessors or persons, anyhow, have them under their control, including system operators. Otherwise, the judge shall issue the order of search and seizure without the presence of the mentioned persons.

Art 38- the search and seizure order must contain the information which aids the accurate execution thereof, including order execution in/out of the location, the qualifications and scopes [limits] of search and seizure, type and extent of the considered data, type and number of the hardware and software, the method of accessing the encrypted or deleted data, and the approximate time needed for accomplishment of search and seizure.

Art 39- Data or computer and telecommunication systems' search and seizure include the following measures:

- Gaining access to computer and telecommunication systems, in whole or in part;
- Gaining access to data carriers including diskettes, compact discs, or memory discs;
- Gaining access to encrypted or deleted data.

Art 40- In data seizure, proportionately considering the type, importance, and role of data in committing crime, methods including data printing, copying or imaging data -in whole or in part, making data inaccessible by means of techniques including changing passwords, encryption, and confiscation seizure of data carriers are practiced.

Art 41- in any of the following cases, the computer or telecommunication systems shall be seized:

- The stored data is not conveniently accessible or is in large volume
- Search, and analysis of data is not possible without having access to the hardware system;
- The legal possessor of data has given his/her consent;
- Copying data is not technically possible;
- In-place search causes damage to data.

Art 42- Seizure of the computer or telecommunication systems is performed proportionately considering their type, importance, and role in committing a crime, and by means of methods including changing passwords to cause lack of access to the system, in-place plumping, and seizure of the system.

Art 43- in case of necessity of seizure of the data relevant to the committed crime existing in other computer or telecommunication systems which are under control or possession of the accused, during seizure process, the officers by the order of the judicial authority- shall expand the width of search and seizure to the mentioned systems, and take actions to search or seize the considered data.

Art 44- Seizure of the data, or computer or telecommunication systems, in the event of causing physical injury or severe economic damages to individuals, or disruption to public services provision, is forbidden.

Art 45- In cases that the original data is seized, the beneficiary is entitled to, after paying the cost, make a copy of them; provided that the presentation of the seized data is not concerned criminal or contrary to the confidentiality of the investigations, and does not affect the procedure thereof.
Art 46- in cases that the original data or computer or telecommunication system are seized, the judge is obligated to, considering the type and volume of data, type, and the number of the considered hardware and software, and their role in committed action, make decisions about them within a reasonable period of time.

Art 47- The affected person is entitled to deliver his/her objection in writing with regard to the actions and measures taken by officers in search and seizure of data and computer and telecommunication systems, along with the reasons of the objection, to the judicial authority issuing the order. The mentioned objection shall be examined out of turn, and the decision shall be appealable.

Title 3- Interception the Content data

Art 48- intercepting the content of non-public communications in transit between computer or telecommunication systems shall be pursuant to the laws and regulations respecting interception of telephone conversations.

Note: Gaining access to the content of stored non-public communications, including e-mail or short message service, is tantamount to intercepting, and necessitates observance of the relevant regulations and laws.

Chapter 3- Admissibility of Digital Evidence

Art 49- For the purpose of protection of the accuracy, integrity, validity, and admissibility of the collected digital evidence, it is necessary to protect hem pursuant to the relevant executive by-laws

Art 50- In the event that the computer data is created, processed, stored, or transferred by the parties of the suit or the third party which unaware of the existence of the suit, while the relevant computer or telecommunication system operates so properly that the accuracy, integrity, validity, and admissibility of data are not affected, the data shall be admissible.

Art 51- All the provisions of the chapter (2) and (3) of this section, shall be applied to other crimes in which digital evidence are referred to, in addition to computer crimes.

Section 3- Miscellaneous Provisions

Art 52- In cases the computer or telecommunication system is used as a means of committing the crime, and there is no punishment provided for the mentioned action, the relevant criminal laws and regulations shall be applicable.

Note: In cases, there are no specific regulations provided in section (2) of the present act respecting the legal procedure of trial of computer crimes, the provisions of the criminal procedure act are applicable.
Art 53- The amounts of fines provided in this act are changeable every three years, based on the official annual inflation rate declared by the central bank, with the recommendation of the chief justice, and ratification of the Board of Ministers.

Art54- Executive by-laws regarding collection and admissibility of digital evidence shall be drafted within 6 months from ratification of the present action by the Ministry of justice, with the cooperation of Ministry of Information and Communication Technology (ICT), ratified by the Ministry of Justice.

Art 55- Articles (1) to (54) of the present act are considered as Articles (726) to (782) of the Iranian Penal Code (Ta'zirat and Deterrent Punishments Section), under the title "Computer Crimes Chapter", and the number of the article (729) of the Penal Code is corrected to (783).

Art 56- Laws and regulations contrary to the present act become invalid.
The above act, consisting of 56 articles and 25 notes, was ratified in the open session of the Islamic Constative Assembly (Majlis) [Parliament of the Islamic Republic of Iran], dated Thursday, Khordad 5, 1388, and confirmed by the Guardian Council on 20/3/1388.[30]

C. Organizations against Cybercrime in Iran

Iranian Cyber Police (FATA Police)

The FATA Police for the Production and Exchange of Information Sphere is an Islamic Republic of Iran Police agency established in January 2011. In 2009, Iran's Police Chief announced plans to set up a cyber police division to counter "Internet crimes".

FATA's activities and responsibilities

In its battle against "cybercrime," FATA is engaged in a variety of distinct operations, with its main objectives being:

- The Internet and other digital systems to monitor and fight cybercrime (i.e. internet scams such as phishing) To monitor the activities of ISPs
- To monitor Internet cafes
- To supervise housing companies and other companies engaged in the data industry
- Collecting and processing Internet usage information and gathering Internet user knowledge
- Informing customers and informing them of cyberspace safety hazards
- • Protecting and maintaining Iran's cultural and domestic heritage
- To prevent violations of societal norms and values

Technical abilities

Generally, Iranian organizations have had problems securing access to skilled workers and technical resources, with FATA being no exception. As a result, the organization often uses unconventional methods to catch cyber criminals, including acts of manipulation on social networking sites. One of the most popular methods used by FATA is the creation of fake Facebook profiles, through which they may encourage other users to divulge personal information. During an investigation, a FATA agent can collect from their social network accounts numerous pieces of information about a user, linking them together to create a completer and more accurate image of the user. [31].

FATA's Central Unit has always communicated with other FATA headquarters across the nation the recent technical studies on surveillance and implementation techniques. Furthermore, this system tries to identify loopholes and zero-day vulnerabilities in Iranian computer devices and software in an attempt to avoid exploitation of safety weaknesses. In addition to this central unit, FATA also consists of several more expert segments, one of which is the Technical Department. Here, a variety of technical employees are regularly trained in Internet and computer networks and safety problems (although most FATA employees are not technically trained). Regardless, FATA claims that its activities are incredibly far-ranging, with FATA's chief in Kerman Province, Kambiz Esmaeili, stating that the organization monitors all activity on websites, blogs and forums on a 24/7 basis. [31]

Organized Crime Investigation Center

The Organized Crime Investigation Center is one of the agencies affiliated with the Revolutionary Guards Intelligence Organization, which was established in 2007.
The purpose of the center is to deal with organized domestic and international movements and abuse of the internet (against the Islamic Republic of Iran) and other communication systems to carry out terrorist acts, cyber-espionage, money laundering and cultural offenses (against the culture of the Islamic Revolution of Iran) and defamation and insult to the sacred religion of Islam and the values of the Islamic Revolution of Iran. This center has been formed in cooperation with the Iranian Judiciary and based on article 150 of the Constitution of the Islamic Republic of Iran to protect this system and its achievements. [32]

Committee for determining the criminal contents

The Committee for Determining the Instances of Criminal Content was established by The Iranian Judicial Administration. It is located at the Office of the State Prosecutor General. Members of this committee are ministers (or their representatives) of the Education, Information and Communication Technology (ICT), intelligence, Justice, Science, Research and Technology, Culture and Islamic Guidance, and the head of the Islamic Republic of Iran Broadcasting, the Commander-in-Chief of the Police, an expert in information and communication technology chosen by the Commission of Industries and Mines of the Iranian parliament and one of the members of the Legal and Judicial Commission of the Islamic Consultative Assembly. The State

Prosecutor General shall be the chairman of the committee. [33]

Ministry of Intelligence

The Islamic Republic of Iran's Ministry of Intelligence is the Islamic Republic of Iran's leading information organization and a part of the Iran Intelligence Community. It's also called VAJA**.** The ministry is one of the three "sovereign" ministerial bodies of Iran due to the nature of its work at home and abroad. It's responsible for the acquisition and development of security intelligence and offshore intelligence, information protection, counterintelligence, and terrorism [34].

The Ministry of Intelligence and Security (MOIS) utilizes all available tools to safeguard Iran's Islamic Revolution, using techniques such as infiltrating inner opposition groups, tracking national attacks and expatriate dissent, capturing suspected spies and dissidents, revealing conspiracies considered dangerous and liaising with other international intelligence agencies as well as with organizations that protect the Islamic Republic's interests in the world [34].

All organisations must exchange data with the Ministry of Intelligence and Security in accordance with Iran's constitution. All clandestine activities are supervised by the ministry. It generally performs inner activities on its own, but for the most portion, the Quds Force of the Islamic Revolutionary Guards Corps performs extraterritorial activities such as harassment, assassinations and spying. Although the Quds Force operates independently, it shares the information it collects with MOIS. [34]

Passive Defense Cyber Division

Duties:

- The cyber defence of the country's fundamental infrastructure base on their level of importance.
- Smart and effective multi-layer defence of the country's cyber assets.
- Command, steer and control the scene of cyber defence operations at national, regional and institutional levels.
- Creating, upgrading and strategizing the country's comprehensive cyber defence system.
- Develop and enhance cyber defence preparedness in the executive, private sector and community sectors.
- Creating, supporting and enhancing the self-reliance capabilities of the country's domestic cyber defence industry.
- Institutionalization of cyber defence concepts in the essence of educational and cultural programs of the country at different levels. [35]

MAHER CERT

Given the importance of responding to information exchange events and setting up cyber disaster response centers in most countries, MAHER CERT has been established as the national CERT of Iran in the year 2008. Since then Maher Center has had the responsibility of countrywide actions for the prevention of and response to such security incidents in information exchange environments.

Scope:

- Rescue and response activities: Immediate investigation of cyberspace incidents based on the request of various organizations.
- Prevention activities: Providing warnings, notifications, risks, and vulnerabilities of nationwide information systems and the publication of guideline packages to strengthen such systems against attacks and other possible incidents.
- Security quality levels improvement activities: Providing workshops and security courses based on current technology trends & needs.

Goals and Duties:

- To provide a central national node for strategic coordination activities in information exchange environments incidents based on the division of work and responsibilities as provided by the high council of cyberspace.
- To build sufficient capacities in order to respond to cyber incidents in the country.
- The exchange of experiences and analysis of incident responses.
- Helping organizations, government centres, and private companies create CSIRT groups.
- Facilitate communication between groups with similar directions and related organizations in order to share knowledge in the cybersecurity field.
- Development of secure communication mechanisms for reliable communication among groups.
- To join in international groups and also the formation of international interaction centres to confront common threats.
- Sharing of important analysis regarding systems' security and important threats on a national level.
- Support for continuous security evaluations in various information exchange environments.
- Knowledge transfer through educational courses.
- Communication and cooperation with other CERTs at national, regional and international levels.

- Holding meetings, seminars, and conferences related to confronting cyber-attacks.
- Cooperation with related organizations with the goal of drafting and passing laws, regulations and policies that affect the capacity to deal with cyber incidents. [36]

D. *Cyber Crime Cases*

Iran-Case 1

Title: DDoS (Distribution Denial of Service)
Related Law:
1: Unauthorized Access (Art.1)
2: Computer Spy (Art.3)
3: Computer Spy (Art.4)
4: Data or Computer or Telecommunication System Interference (Art.9)
5: Computer Related Theft and Fraud (Art.13)

Case detail:

DDoS or distribution denial of service is one of the most common cyber-attacks targeting the servers of a service provider. A DDoS attack occurs when a large number of false requests are sent to the server intentionally to flood that server. If you ever visited a website to buy a ticket or product at a limited time with too many users at the same time, you may have noticed that a large number of demands slow or even crash the server. In such cases, server failure is deliberated, but in DDoS attacks, this is occurring intentionally. The purpose of such attacks is to crash the particular website or sometimes to disturb the site administrator to make the site inaccessible. Typically, a DDoS attack can be managed. If the server finds that too many demands are coming from the IP which directs the attack, it would be able to stop that by closing access requests from the location or IP address [37].

It should be mentioned that it is not the first time that Iranian websites have been faced with this attack. At the beginning of 2016, some payment terminals such as Zarrin-Pal, Mehr-Pal, Azad Pay were hit by this attack. In the same year, one of the biggest attacks against Digikala's online payment portal was attacked for 45 hours, and it reached to 79 gigabits per second. In summer 2017, banking systems were targeted again, and in the most recent event, more than 20 online businesses in the country were hit by DDoS.
According to the CEO of Zarrin-Pal company, the origins of this attack is not clear yet, but part of the attacks came from outside the country and from European data centers, and the other part was carried out from inside of Iran [37].

Each attack is done on a specific purpose. In the case of recent attacks on online business websites, hackers have requested for Bitcoin as ransom, and sometimes executives of these websites and their families have been threatened through a telegram account called Master.
The aim of this attack was to receive Bitcoin. At first, the hacker asked for half of a Bitcoin, and when he did not get any response, he increased the amount of attacks on the website and then requested 5 Bitcoin. Finally, in a call with FATA Police, he said that if they wanted to stop the attack, they would have to pay 10 Bitcoin. By December of that year, Bitcoin was worth about $10000 worth [37].

The role of Iranian Patches for Telegram in DDoS attacks:

So far, internet services such as Master Blit, ITP, Gift-Card, have been attacked. As mentioned, these kinds of attacks have two sources, domestic and foreign. The scope of the DDoS attack is not limited to online businesses. According to the investigations by MAHER CERT, part of the external attacks were done by European data centers, and are trying to control or reduce the impact of attacks, but for the domestic ones, after analysis done by MAHER CERT, it was determined the attacks came from the IP addresses which belong to Mobile Operators within Iran, so it illustrates that some malwares are being unintentionally installed on people cellphones [37].
After reaching to this fact that the infected applications were the cause of the attacks, some cybersecurity experts suggested that presumably, Iranian patches for Telegram application were one of those infected apps. By filtering the Telegram application, many Iranian users are using these patches, which are considered legal proxies (using proxies in Iran is illegal), to bypass filtering. Since last months, before the prevalence of these patches, the Ministry of Communications warned against the security problems of these patches [37].

Sentences [37]:

- Every person who, without authority, gains access to data, or computer or telecommunication systems which are protected under security measures shall be punished by a term of 91 days to 1 year of imprisonment, or by a fine of 5,000,000 to 20,000,000 Rials, or by both the imprisonment and fine.
- Gaining access to the aforesaid data or acquisition of them, or interception the content of the secret data in transit; by a term of 1 to 3 years of imprisonment, or by a fine of 20,000,000 to 60,000,000 Rials, or by both the imprisonment and fine;
- Making the aforesaid data accessible to unauthorized persons; by a term of 2 to 10 years of imprisonment;
- Disclosure of the aforesaid data or making them accessible to a foreign government, organization,

corporation, or group, or their agents, by a term of 5 to 15 years of imprisonment

- Every person who, without authority, disables another person's computer or telecommunication systems, or disturbs their function by inputting, transmitting, distribution, deleting, suppressing, manipulation, or deterioration of data or electromagnetic or optical waves shall be punished by a term of 6 months to 2 years of imprisonment, or by a fine of 10,000,000 to 40,000,000 Rials, or by both the imprisonment and fine.
- Every person who, without authority, disables another person's computer or telecommunication systems, or disturbs their function by inputting, transmitting, distribution, deleting, suppressing, manipulation, or deterioration of data or electromagnetic or optical waves shall be punished by a term of 6 months to 2 years of imprisonment, or by a fine of 10,000,000 to 40,000,000 Rials, or by both the imprisonment and fine.
- Every person who, with the intent to access the secret data provided in article 3 of the present act, violates the security measures of the computer or telecommunication systems shall be punished by a term of 6 months to 2 years of imprisonment, or by a fine of 10,000,000 to 40,000,000 Rials, or by both the imprisonment and fine.

Iran-Case2:

Title: Phishing and Fraud
Related Law:
1: Unauthorized Access (Art.1)
2: Computer Spy (Art.3)
3: Computer Related Theft and Fraud (Art.12)
4: Computer Related Theft and Fraud (Art.13)

Case detail:

The young man was arrested twice in the last three years, he was in charge of hacking and thievery of bank accounts from various provinces. The Tenty-four years old man said that he is the resident of Alborz Province. Each time he released after his imprisonment he began his criminal acts again. Whenever he was arrested, he chose a safer way to steal from his victims' accounts. This time, he tried to reduce being identified and then captured by FATA Police, but again, he was unfortunate. FATA Police detectives were conducted to track down the young hacker following the complaint filed by one of the victims. The man claimed that:" I was surprised when I received my bank statement from the bank. I realized that a large amount of money withdrawn from my account. At first, I thought that it was a mistake, but the bank employee said that this amount was taken online from my account "[38]. By receiving a complaint from the victim to track down the perpetrator, officers started doing some investigations. While FATA investigators have been started to trace the footprint of the hacker, they received similar reports from several banks in other provinces that same cases happened there. In all of those cases, the hacker began to infiltrate his victims account by using malware and other combined methods. The method of infiltration indicated that the hacker was very professional and used a combination of methods to get to his goal [38].

Arrest and interview:

The chief police officer of Alborz province explained that following a complaint of the man whose account was being hacked, by using forensic tools and data provided by ISPs to trace the IP address of the hacker, investigators could locate the physical address of him [38].
When the police arrived at his place, he still did not make his last victim's account empty. So, the evidence was in plain sight and implied charges against him. When he was arrested, during his preliminary interrogation, he claimed that he had been unaware of the fact that all the money from bank accounts were had been withdrawn and he had done it only because of curiosity. After facing undeniable facts and pieces of evidence that being presented by FATA police investigators, he admitted being guilty [38].
During investigations, it was found that he was arrested two times in the past three years for the same crime. The hacker attempted to create keylogger spyware. By publishing it in the social media or by sending an infected email in the format of photo, music, software. This malware was entered into the victim's systems. The malware was running on infected computers to send the card and password code (CVV2) and other victim account information to the hacker's personal email, and in a proper occasion, he started to transfer money to fake accounts he made for himself and lastly purchasing gold and jewelry with it across Iran [38].
Before identifying and interviewing the hacker, the law enforcement officers arrested him in a surprise raid, and he confessed that he held bank account information of thousands of people and possessing their personal data such as their private pictures, emails, username and password of another social media, etc. [38].

Lesson Learned:

The officer who was in charge of the case suggested some recommendations to prevent such cases happening in future:

- When doing online banking, try to enter your personal information through the portal that the bank provides to the user, to avoid being the next victims of these type of attacks.
- When you are doing online purchasing or other online transactions, enter your account information randomly. In case that you have been targeted to such kind of attacks.
- Do not open the spams (unknown emails) received in your email. They might have keylogger malware.

- Always monitor your traffic; generally, inbound traffic must be less than outbound traffic. If you observe a suspicious change in your traffic, notify someone who is expert in this material.
- To access your personal accounts, never use public computers. Otherwise, you will increase the possibility of being targeted by the keyloggers. [38]

Sentences [38]:

- Every person who, without authority, gains access to data, or computer or telecommunication systems which are protected under security measures shall be punished by a term of 91 days to 1 year of imprisonment, or by a fine of 5,000,000 to 20,000,000 Rials, or by both the imprisonment and fine.
- Every person who, without authority, commits any of the following acts against stored or in transit secret data in storage media or computer or telecommunication systems shall be punished by the provided punishments:
- Gaining access to the aforesaid data or acquisition of them, or interception the content of the secret data in transit; by a term of 1 to 3 years of imprisonment, or by a fine of 20,000,000 to 60,000,000 Rials, or by both the imprisonment and fine;
- Making the aforesaid data accessible to unauthorized persons; by a term of 2 to 10 years of imprisonment;

- Every person who, without authority, thievery of data belonging to others, while the original data remains, shall be punished by a fine of 1,000,000 to 20,000,000 Rials, and otherwise, by a term of 91 days to 1 year of imprisonment, or by a fine of 5,000,000 to 20,000,000 Rials, or by both the imprisonment and fine.
- Every person who, without authority, obtains money, property, profits, services, or financial advantages for himself or another person, by committing acts, including entering, altering, deleting, creating, suppression data, or disturbing the system shall be punished by a term of 1 to 5 years of imprisonment, or by a fine of 20,000,000 to 100,000,000 Rials, or by both the imprisonment and fine, in addition to restitution of the property.

Iran-Case 3:

Title: Phishing and Fraud
Related Law:
1: 1: Unauthorized Access (Art.1)
2: Computer Spy (Art.3)
3: Computer Related Theft and Fraud (Art.12)
4: Computer Related Theft and Fraud (Art.13)

Case detail:

A man who was tricking people into installing unauthorized applications and then defrauded them was arrested by Mazandaran FATA police cybercrime detectives.
Iran cybercrime police chief said:" the victim who was one of the Mazandaran residence referred to the police station and stated that in a telegram group that had predicted football matches, I met a person who introduced himself as "Soheil". After a while, He suggested he deposits some money into my account to buy him a voucher code and pay 100000 Rials as a commission per every 1000000 rials to me. So, I started to buy some voucher code for him, which eventually various people called me and claimed that some money had been withdrawn from their accounts and deposited into my account" [39]. He added:" according to the complaint, and with the cooperation of judicial officer, the investigations on this case started to be followed. During the investigations, it was determined that in addition to the mentioned victim, the accused person did the other people bank accounts robbery as well "[39].
Furthermore, he continued:" some other people came to the FATA police stations and claimed that some money had been deposited to their accounts to buy the voucher. By examining the police investigators, it revealed that the accused deposited the stolen amount of money to their bank accounts while they were unaware of the matter and had been abused by the accused "[39].
Finally, FATA police officers identified the main defendant of the case who was living in one of the Tehran provinces committed these types of the crime of unauthorized withdrawal from people bank accounts in the past. The FATA police officer added: police arrested the accused with the arrest warrant in his residence and seized some number of bank cards with computer and telecommunication systems in his home. By ordering of prosecutor, the accused was referred to the Mazandaran FATA police. During the investigations, while he confessed his imputed victim, he declared that after being released from the prison in September 2016, he had designed the program called" Pocket Satellite and Satellite Finders." Since March of that year, and with communication with admins of telegram who had a high number of followers, he requested advertising of his own designed program in exchange for paying some amount of money to them.
He continued:" after installing apps by users, they had to pay 20000 Rials to activate the program, directing users to the fake banking portal, sending their bank account information to the accused through a telegram robot he had created, then he proceeded to withdraw money from users account, transferred theft money to the different people accounts, requested to buy vouchers by giving commissions to them, bet on online gambling sites, he transferred the amount of money received from these sites to the bank card he bought from an addicted person in exchange of 1000000 Rials and then he withdrew it [39].
The police officer mentioned:' according to the investigations carried out by FATA police officers, 300 bank card numbers

belonging to different people were identified which were frauded and the accused was sent to court for prosecution.
Nowadays, many unauthorized programs in cyberspaces are counted as prey for fraudsters said the chief of the Mazandaran Fata police. He suggested some recommendation to prevent or minimize such kinds of cybercrimes:

- Users should be careful not to trust any program that is advertised on the internet because these could be tricky to bring the users to the fake portals and make frauds through that.
- According to the law, gambling is based on articles 705- 708-710-780 of the Islamic Penal Code is recognized as a crime, and what gamblers and gambling establishers are guilty, and they will be prosecuted. [39]

Sentences [39]:

- Every person who, without authority, gains access to data, or computer or telecommunication systems which are protected under security measures shall be punished by a term of 91 days to 1 year of imprisonment, or by a fine of 5,000,000 to 20,000,000 Rials, or by both the imprisonment and fine.
- Every person who, without authority, commits any of the following acts against stored or in transit secret data in storage media or computer or telecommunication systems shall be punished by the provided punishments:
- Gaining access to the aforesaid data or acquisition of them, or interception the content of the secret data in transit; by a term of 1 to 3 years of imprisonment, or by a fine of 20,000,000 to 60,000,000 Rials, or by both the imprisonment and fine;
- Making the aforesaid data accessible to unauthorized persons; by a term of 2 to 10 years of imprisonment;
- Every person who, without authority, thievery of data belonging to others, while the original data remains, shall be punished by a fine of 1,000,000 to 20,000,000 Rials, and otherwise, by a term of 91 days to 1 year of imprisonment, or by a fine of 5,000,000 to 20,000,000 Rials, or by both the imprisonment and fine.
- Every person who, without authority, obtains money, property, profits, services, or financial advantages for himself or another person, by committing acts, including entering, altering, deleting, creating, suppression data, or disturbing the system shall be punished by a term of 1 to 5 years of imprisonment, or by a fine of 20,000,000 to 100,000,000 Rials, or by both the imprisonment and fine, in addition to restitution of the property.

TURKEY

A.Legal and Judicial System in Turkey

Turkey's judiciary has been fully incorporated into continental Europe's scheme. The Turkish Civil Code, for example, has been amended by integrating aspects of the Swiss Civil Code (Civil Law) and Code of Obligations and the German Commercial Code in particular. There are differences between the Administrative Code and its French equivalent, and the Penal Code and its Italian version.
Turkey's judicial system is described by Articles 138 to 160 of the Constitution of 1982. There is separate civil and army jurisdiction. While military tribunals generally only attempt army staff, soldiers can also be tried in martial law and military service matters [82].

Scope of Turkish Judicial System

- The Ministry of Justice: Has an important role within Turkish judicial system and is responsible for determining the main policies about the system as well as controlling the budgets of important bodies within this system.
- The High Council of Judges and Prosecutors: Is an independent supreme board that is established to act in accordance with the principles of independence of courts and tenures of judges and prosecutors. Its establishment purpose is to make decisions on appointment, promotions and assignments of those working under the judge class.
- Supreme Courts: Turkey has supreme courts, rather than one supreme court, because of its multipartite structured judicial system. These supreme courts are the final decision-making authorities in the fields of civilian, administrative and military judiciary. These courts are The Constitutional Court, The Court of Cassation, The Council of State, The Military Court of Cassation, The High Military Administrative Court, and The Court of Jurisdictional Disputes.
- District Courts: In Turkey, district courts are found only in civilian judiciary branch. These courts evaluate the appeal applications against the decisions of the first instance courts and act as the first instance court in some cases with special nature as well. These courts are Ordinary and Administrative Courts, Military Courts.
- First Instance Courts: First instance courts are trial courts established to deal with the cases at the first stage. In Turkey, three types of first instance courts are established on the basis of jurisdictional separation of civilian – military jurisdictions and ordinary – administrative jurisdictions.
- The Supreme Election Boards and Other Boards: Turkish Constitution ensures that elections will be carried out under the general management and inspection of the judicial bodies. In election boards, judges serve in decision-making positions, however these boards are completely independent from the courts in terms of both their structure and decisions.

- Justice Institutions for Enforcement of Judgements: Two different types of justice institutions have been established to enforce the judgements of courts; prisons and detention houses in terms of criminal law judgments and directorates of enforcement and bankruptcy in terms of civil law judgements.

Legal System

Secularism is a component of the law of Turkey. Turkey's first chairman, Mustafa Kemal Atatürk, set the administrative and political criteria for a contemporary, representative, secular Kemalist country [32]. The legal system is civil law (and not common law), the power of court decisions is limited, and these are not regarded as a main source of law. Accordingly, although prior higher court decisions can guide judges in the decision-making process, they are not binding and can be disregarded when reaching a conclusion in the case at hand. However, the decisions of the Court of Appeal's General Assembly on the Unification of Judgments. are binding on judges. This is not a separate appellate body but an assembly of the Court of Appeal which renders decisions regarding points of laws on which its different chambers disagree [83].

B. Turkish Cyber Crime Laws

Substantive Criminal Laws
All laws are mentioned according to website of Council of Europe [58]

Illegal access
Accessing a data processing system
Article 243 - (1) Any person who unlawfully accesses, partially or fully, a data processing system, or remains within such system, shall be subject to a penalty of imprisonment for a term of up to one year or a judicial fine.
(2) Where the act defined in the aforementioned paragraph is committed in relation to a system which is only accessible upon the payment of a fee, then the penalty to be imposed shall be decreased by up to one half.
(3) Where any data within any such system is deleted or altered as a result of this act, then the penalty to be imposed shall be a term of imprisonment of six months to two years.
(4) (Additional: 24/3/2016-6698/Article 30) A person who monitors data transfers within a data processing system or among data processing systems by means of technical equipment without accessing the system shall be imposed a term of imprisonment of one year to three years.
Preventing the functioning of a system and deletion, alteration or corrupting of data
Article 244 - (1) Any person who prevents the functioning of a data processing system or renders it useless shall be subject to a penalty of imprisonment for a term of one to five years.
Any person who deletes, alters, corrupts or bars access to data, or introduces data into a system or sends existing data to another place
shall be subject to a penalty of imprisonment for a term of six months to three years.
(3) Where such acts are committed in relation to a data processing system of a bank or credit organization, or of a public institution
or establishment, then the penalty to be imposed shall be increased by one half.
(4) Where a person obtains an unjust benefit for himself or another by committing the acts defined in the aforementioned paragraphs, and such acts do not constitute a separate offence, he shall be subject to a penalty of imprisonment from two years to six years and a judicial fine of up to five thousand days.

Illegal interception
Accessing a data processing system
Article 243 - (1) Any person who unlawfully accesses, partially **or** fully, a data processing system, or remains within such system, shall be subject to a penalty of imprisonment for a term of up to one year or a judicial fine.
(2) Where the act defined in the aforementioned paragraph is committed in relation to a system which is only accessible upon the payment of a fee, then the penalty to be imposed shall be decreased by up to one half.
(3) Where any data within any such system is deleted or altered as a result of this act, then the penalty to be imposed shall be a term of imprisonment of six months to two years.
(4) (Additional: 24/3/2016-6698/Article 30) A person who monitors data transfers within a data processing system or among data processing systems by means of technical equipment without accessing the system shall be imposed a term of imprisonment of one year to three years.

Data interference
Accessing a data processing system
Article 243 - (1) Any person who unlawfully accesses, partially **or** fully, a data processing system, or remains within such system, shall be subject to a penalty of imprisonment for a term of up to one year or a judicial fine.
(2) Where the act defined in the aforementioned paragraph is committed in relation to a system which is only accessible upon the payment of a fee, then the penalty to be imposed shall be decreased by up to one half.
(3) Where any data within any such system is deleted or altered as a result of this act, then the penalty to be imposed shall be a term of imprisonment of six months to two years.
(4) (Additional: 24/3/2016-6698/Article 30) A person who monitors data transfers within a data processing system or among data processing systems by means of technical equipment without accessing the system shall be imposed a term of imprisonment of one year to three years.
Preventing the functioning of a system and deletion, alteration or corrupting of data

Article 244 - Any person who deletes, alters, corrupts or bars access to data, or introduces data into a system or sends existing data to another place shall be subject to a penalty of imprisonment for a term of six months to three years

System interference
Accessing a data processing system
Article 243 - (1) Any person who unlawfully accesses, partially **or** fully, a data processing system, or remains within such system, shall be subject to a penalty of imprisonment for a term of up to one year or a judicial fine.
(2) Where the act defined in the aforementioned paragraph is committed in relation to a system which is only accessible upon the payment of a fee, then the penalty to be imposed shall be decreased by up to one half.
(3) Where any data within any such system is deleted or altered as a result of this act, then the penalty to be imposed shall be a term of imprisonment of six months to two years.
(4) (Additional: 24/3/2016-6698/Article 30) A person who monitors data transfers within a data processing system or among data processing systems by means of technical equipment without accessing the system shall be imposed a term of imprisonment of one year to three years.
Preventing the functioning of a system and deletion, alteration or corrupting of data
Corresponding article in the legislation
Turkish Penal Code 244/1,3,4.
Preventing the functioning of a system and deletion, alteration or corrupting of data
Article 244 - Any person who prevents the functioning of a data processing system or renders it useless shall be subject to a penalty of imprisonment for a term of one to five years.
Where such acts are committed in relation to a data processing system of a bank or credit organization, or of a public institution, then the penalty to be imposed shall be increased by one half.
Where a person obtains an unjust benefit for himself or another by committing the acts defined in the aforementioned paragraphs, and such acts do not constitute a separate offence, he shall be subject to a penalty of imprisonment from two years to six years and a judicial fine of up to five thousand days.

Misuse of devices
Turkish Penal Code a.243, a.244, a.245, 245/A
Accessing a data processing system
Article 243 - (1) Any person who unlawfully accesses, partially **or** fully, a data processing system, or remains within such system, shall be subject to a penalty of imprisonment for a term of up to one year or a judicial fine.
(2) Where the act defined in the aforementioned paragraph is committed in relation to a system which is only accessible upon the payment of a fee, then the penalty to be imposed shall be decreased by up to one half.
(3) Where any data within any such system is deleted or altered as a result of this act, then the penalty to be imposed shall be a term of imprisonment of six months to two years.
(4) (Additional: 24/3/2016-6698/Article 30) A person who monitors data transfers within a data processing system or among data processing systems by means of technical equipment without accessing the system shall be imposed a term of imprisonment of one year to three years.
Preventing the functioning of a system and deletion, alteration or corrupting of data
Article 244 - (1) Any person who prevents the functioning of a data processing system or renders it useless shall be subject to a penalty of imprisonment for a term of one to five years.
Any person who deletes, alters, corrupts or bars access to data, or introduces data into a system or sends existing data to another place
shall be subject to a penalty of imprisonment for a term of six months to three years.
(3) Where such acts are committed in relation to a data processing system of a bank or credit organization, or of a public institution
or establishment, then the penalty to be imposed shall be increased by one half.
(4) Where a person obtains an unjust benefit for himself or another by committing the acts defined in the aforementioned paragraphs,
and such acts do not constitute a separate offence, he shall be subject to a penalty of imprisonment from two years to six years and a judicial fine of up to five thousand days.

Misuse of bank or credit cards
Article 245 - (Amended: 29/6/2005 – 5377/Article 27)
(1) If any person who acquires or retains a bank or credit card of another person secures a benefit for himself or another person by using or allowing the use of such cards without the consent of the card holder or the person to whom the card should be given, he shall be sentenced to a penalty of imprisonment for a term of three to six years and a judicial fine of up to five thousand days.
(2) Any person who produces, sells, transfers, purchases or receives a counterfeit bank or credit card related to the bank accounts of another person shall be sentenced to a penalty of imprisonment for a term of three years to seven years and imposed a judicial fine of up to ten thousand days.
(3) Any person who secures a benefit for himself of another person by using a counterfeit or falsified bank or credit card shall be sentenced to a penalty of imprisonment for a term of four to eight years and imposed a judicial a fine of up to five thousand days provided that the act does not constitute another offence that is punishable by a heavier penalty.
(4) Where an offence specified in paragraph one damages
a) a spouse of a marriage where a court decree of separation has not been made,
b) a direct-ascendant or direct-descendant, direct in-law, adoptive parent or adopted child, or
c) one of the siblings residing in the same dwelling,
the relevant relative shall not be subject to a penalty.
(5) (Additional: 6/12/2006 – 5560/Article 11) Effective repentance provisions related to offences against property

under this Law shall be applicable to the acts included in the scope of the paragraph one.

Prohibited devices or programs

Article 245/A - (Additional: 24/3/2016-6698/Article 30)

If a device, computer program, encryption or any other security code is made or created exclusively for committing the offences specified in this Section and any other offence committed by means of data processing systems, those who produce, import, transport, store, receive, sell, expose for sale, purchase, give another person or keep them shall be sentenced to a penalty of imprisonment for a term of one year to three years and imposed a judicial fine of up to five thousand days.

Law no. 5846 on Intellectual and Artistic Works (LIAW)

Article 72 - (Amended: 23/1/2008-5728/Article 139)

Any person, who produces, puts up for sale, sells or possesses for non- private use any programs and technical equipment which aim to circumvent additional programs developed to prevent illegal reproduction of a computer program shall be sentenced to imprisonment from six months to two years.

Computer-related forgery

Turkish Penal Code a.243, a.244, 204, 207, 244/2

Accessing a data processing system

Article 243 - (1) Any person who unlawfully accesses, partially **or** fully, a data processing system, or remains within such system, shall be subject to a penalty of imprisonment for a term of up to one year or a judicial fine.

(2) Where the act defined in the aforementioned paragraph is committed in relation to a system which is only accessible upon the payment of a fee, then the penalty to be imposed shall be decreased by up to one half.

(3) Where any data within any such system is deleted or altered as a result of this act, then the penalty to be imposed shall be a term of imprisonment of six months to two years.

(4) (Additional: 24/3/2016-6698/Article 30) A person who monitors data transfers within a data processing system or among data processing systems by means of technical equipment without accessing the system shall be imposed a term of imprisonment of one year to three years.

Preventing the functioning of a system and deletion, alteration or corrupting of data

Article 244 - (1) Any person who prevents the functioning of a data processing system or renders it useless shall be subject to a penalty of imprisonment for a term of one to five years.

Any person who deletes, alters, corrupts or bars access to data, or introduces data into a system or sends existing data to another place

shall be subject to a penalty of imprisonment for a term of six months to three years.

(3) Where such acts are committed in relation to a data processing system of a bank or credit organization, or of a public institution

or establishment, then the penalty to be imposed shall be increased by one half.

(4) Where a person obtains an unjust benefit for himself or another by committing the acts defined in the aforementioned paragraphs,

and such acts do not constitute a separate offence, he shall be subject to a penalty of imprisonment from two years to six years and a judicial fine of up to five thousand days.

Counterfeiting official documents

Article 204 - (1) Any person who issues a counterfeit official document, alters a genuine official document to deceive others or uses a counterfeit official document shall be sentenced to a penalty of imprisonment from two years to five years.

(2) Any public officer who issues a counterfeit official document that he is authorized to issue, or alters a genuine official document to deceive others, issues a document that does not reflect the truth or uses a counterfeit official document shall be sentenced to a penalty of imprisonment from three years to eight years.

(3) If the official document remains valid by operation of law until it is proven otherwise, the penalty to be imposed shall be increased by one half.

Counterfeiting private documents

Article 207 - (1) Any person who issues a counterfeit private document or alters a and uses a genuine private document in order to deceive others shall be sentenced to a penalty of imprisonment from one year to three years.

(2) Any person who knowingly uses a counterfeit private document shall be punished in accordance with the provisions of the aforementioned paragraph.

Preventing the functioning of a system and deletion, alteration or corrupting of data

Article 244 - (2) Any person who deletes, alters, corrupts or bars access to data, or introduces data into a system or sends existing data to another place shall be subject to a penalty of imprisonment for a term of six months to three years

Computer-related fraud

Corresponding article in the legislation

Turkish Penal Code 158/1. f; 243/ Article 2

Article 158- (1) Where the offence of swindling is committed;

f) with the data processing systems, bank or credit organizations used as an instrument, Misuse of bank or credit cards

Accessing a data processing system

Turkish Penal Code 243/2

(2) Where the act defined in the aforementioned paragraph is committed in relation to a system which is only accessible upon the payment of a fee, then the penalty to be imposed shall be decreased by up to one half.

Offences related to child pornography

Turkish Penal Code

Obscenity

Article 226 - (1) a) Any person who gives a child any material that includes obscene images, texts or words or makes a child watch, read or listen the content of such materials,
b) Shows or publicly exhibits the contents of such materials in places that are accessible to children, or reads, make others read, say or make others say such contents,
c) Offers such materials for sale or rent in such a manner that reveals the contents of such materials,
d) Offers such materials for sale or rent in any place other than those dedicated to the sale thereof,
e) Gives or distributes such material free of charge with the sale of any product or service,
f) Advertises such products, shall be sentenced to a penalty of imprisonment for a term of six months to two years and a judicial fine.
(2) Any person who broadcasts or mediates the broadcast of obscene images, texts or words by press or media organs shall be sentenced to a penalty of imprisonment for a term of six months to three years and a judicial fine of up to five thousand days.
(3) Any person who uses children, representative images of children or those who look like children in producing materials that contain obscene images, texts or words shall be sentenced to a penalty of imprisonment for a term of five years to ten years and imposed a judicial fine of up to five thousand days. Any person who conveys such materials into the country, who copies or offers for sale such material or who sells, transports, stores, exports, retains possession of such material or offers such material for the use of others shall be sentenced to a penalty of imprisonment for a term of two years to five years and imposed a judicial fine of up to five thousand days.
(4) Any person who produces, conveys into the country, offers for sale, sells, transports, stores or offers for the use of others any materials containing text, sounds or images of sexual acts performed by brutal means, or on animals, human corpses, or in any other unnatural manner shall be sentenced to a penalty of imprisonment for a term of one year to four years and imposed a judicial fine of up to five thousand days.
(5) Any person who broadcasts or mediates the broadcast of the contents of materials specified in paragraphs three and four by press or media organs, or causes children to watch, listen or read such materials shall be sentenced to a penalty of imprisonment for a term of six years to ten years and a judicial fine of up to five thousand days.
(6) Legal entities shall be subject to specific security measures for involvement in these offences.
(7) The provisions of this article shall not be applicable to scientific works, and with the exception of paragraph three, to the works of artistic and literary value.
Definitions
Article 6 - (1) In the implementation of criminal laws;
b) Minor shall mean any person under the age of eighteen,
Child sexual abuse

Article 103 - (1) Any person who sexually abuses a child shall be sentenced to an imprisonment from eight years to fifteen years. If the sexual abuse is limited to the level of sexual disturbance, a penalty of imprisonment from three years to eight years shall be applicable. If the offence that is limited to sexual disturbance is committed by a minor, investigation and prosecution shall depend on the complaint of the victim's guardians or custodians. Sexual abuse covers the following acts; (1)
a) Any sexual act towards children who are under the age of fifteen or towards those who attained the age of fifteen but lack the ability to understand the legal meaning and consequences of such act,
b) Sexual acts towards other children by force, threat or on the grounds that affect the will.
(2) If the sexual abuse is committed by inserting an organ or an object into a body, a term of imprisonment that is not less than sixteen years shall be imposed. (2)
(3) If the offence is committed;
a) together by more than one person,
b) by taking advantage of environments where people have to live together,
c) against a person within the first three degrees of kinship or kinship by marriage, or by a stepfather, stepmother, stepsibling or an adoptive parent,
d) by the child's guardian, tutor, instructor, caregiver, custodial parents or by those who provide the child with health care or are under an obligation to protect, look after or supervise the child,
e) by the abuse of the influence provided by the public office or service relationship,
the penalty to be imposed in according to the above paragraphs shall be increased by one half.
(4) If the sexual abuse is committed by force or threat against the children specified in the item (a) of the paragraph one, or by the use of arms against the children specified in the item (b) of the paragraph one, the penalty to be imposed in according to the above paragraphs shall be increased by one half.
(5) In case of use of force and violence during sexual abuse in such a way that results in severe consequences of intentional injury, the provisions related to intentional injury shall also be applicable.
(6) If the victim enters vegetative state or dies as a result of the offence, the offender shall be sentenced to aggravated life imprisonment.

Offences related to infringements of copyright and related rights
LAW NO. 5846 ON INTELLECTUAL AND ARTISTIC WORKS
Corresponding article in the legislation
The Law no. 5846 on Intellectual and Artistic Works, Articles 1/B, 2, 71, 72, 73, 75
Article 71 – (Amended: 23/1/2008-5728/Article 138)

Any person who, by violating the moral, economic and related rights regarding intellectual and artistic works protected under this Law:
1. Processes, represents, reproduces, alters, distributes, publishes by means of instruments that transmit audio or video, broadcasts a work, performance, phonogram, or production, or offers for sale, sells, propagates by renting or lending or by any other means, purchases for commercial purposes, imports or exports, retains for non-personal use or stores a work that is illegally processed or reproduced, shall be sentenced to imprisonment from one year to five years or imposed a judicial fine.
2. Titles another person's work as his own shall be sentenced to imprisonment from six months to two years or imposed a judicial fine. If this act is committed by distributing or broadcasting, the offender shall be sentenced no more than five years of imprisonment, and no judicial fine shall be imposed.
3. Cites from a work without referring to the source shall be sentenced to imprisonment from six months to two years or imposed a judicial fine.
4. Makes a declaration to the public without the permission of its right-holders about a work that has not yet been made public, shall be sentenced to imprisonment up to six months.
5. Gives an incomplete, wrong or misleading reference with regard to a work, shall be sentenced to imprisonment for up to six months.
6. Reproduces, distributes, publishes or broadcasts a work, performance, phonogram or a production by using the name of another well-known other person shall be sentenced to imprisonment from three months to one year or imposed a judicial fine.
Any person who commits the acts mentioned in the paragraph one of the additional articles 4 of this Law and data service providers who continue to violate the rights provided by this Law shall be sentenced to imprisonment from three months to two years, provided that their acts do not constitute an offence that is punishable by a heavier penalty.
If a person who offers for sale, sells or purchases a work, performance, phonogram or production that is processed, reproduced, distributed or broadcast illegally, reports the person from whom he obtained such materials and enables them to be captured before the stage of prosecution, the penalty to be imposed to the former may be reduced or omitted.
2. Preparatory acts for circumventing protective programs (2)
Article 72 - (Amended: 23/1/2008-5728/Article 139)
Any person, who produces, puts up for sale, sells or possesses for non- private use any programs and technical equipment which aim to circumvent additional programs developed to prevent illegal reproduction of a computer program shall be sentenced to imprisonment from six months to two years.
3. Other offences:
Article 73 - (Amended: 23/1/2008-5728/Article 578)
(1) While the title of this article was "1. Violation of moral rights:", it was amended as written in the document by the Article 138 of the Law no. 5728 dated 23/1/2008.
(2) While the title of this article was "2. Violation of financial rights:", it was amended as written in the document by the Article 139 of the Law no. 5728 dated 23/1/2008.
II-Investigation and prosecution (1)
Article 75- (Amended: 23/1/2008-5728/Article 140)
Investigation and prosecution for the crimes mentioned in the articles 71 and 72 shall be subject to complaint. Documents and other evidence proving the rights of the right holders or the professional unions that they are affiliated with shall be submitted to the public prosecutor in order for the complaints filed to be valid. In case of failure to submit such documents and evidence to the public prosecutor within the period of the complaint, a decision of non-prosecution shall be made.
The holders of moral and economic rights on works shall be notified for the case by the relevant natural and corporate entities including primarily the authorities of the Ministry of National Education and Ministry of Culture and Tourism in order to enable the right holders to exercise their rights to complaint.
Upon the complaint, the public prosecutor shall carry out the necessary procedures for confiscation of the property subject to the crime pursuant to Code no. 5271 of Criminal Procedure. Where the public prosecutor deems necessary, he may also order the activity restricted to reproduction of the works that are claimed to be reproduced illegally to be discontinued. However, this order shall be submitted to the approval of the judge within twenty-four hours. An order that is not approved by the judge within twenty-four hours shall be void.

Procedural Criminal Laws
Expedited preservation of stored computer data
Corresponding article in the legislation:
Article 6/1 (b) of the Law no. 5651
ARTICLE 6- (1) Access provider;
b) To retain all traffic data about the services that it provides as specified in the regulations for the period specified in the regulation which cannot be less than six months and more than two years and to maintain accuracy, integrity and confidentiality of such data,

Expedited preservation and partial disclosure of traffic data
Article 6/1 (b) of the Law no. 5651
ARTICLE 6 - (1) Access provider;
b) To retain all traffic data about the services that it provides as specified in the regulations for the period specified in the regulation which cannot be less than six months and more than two years and to maintain accuracy, integrity and confidentiality of such data,

Production order
Article 6/1 (b) of the Law no. 5651
ARTICLE 6 - (1) Access provider;

b) To retain all traffic data about the services that it provides as specified in the regulations for the period specified in the regulation which cannot be less than six months and more than two years and to maintain accuracy, integrity and confidentiality of such data

Search and seizure of stored computer data
Code No. 5271 on Criminal Procedure
Search, copy and seizure of computers, computer programs and logs

Where there are strong reasons for suspicion based on concrete evidence and it is not possible to obtain evidence by other means during the investigation performed for a crime, the judge shall issue, upon the motion of the public prosecutor, a decision on searching of computers, computer programs and computer logs used by the suspect, and on making copies of computer records, and decryption of such records into text.

Where it is not possible to access a computer, computer program, computer logs or hidden data as the passwords are not known, such equipment may be seized to solve the passwords and take necessary copies. Seized devices shall be returned without delay if the passwords are solved and necessary copies are made.

(3) All data on the system shall be backed up during the seizure of computers and computer logs.

(4) A copy of the backup taken in accordance with the paragraph three shall be given to the suspect, and this shall be recorded and signed.

(5) It is also permissible to produce a copy of the entire data or some of the data included on the system, without seizing the computer or the computer logs. Copied data shall be printed on paper and this shall be recorded and signed by the relevant persons

Real-time collection of traffic data
Code No. 5271 on Criminal Procedure
Location, listening and recording of communication

Article 135 – (1) **(Amended: 21/2/2014 - 6526/Article 12)** Where there are strong reasons for suspicion based on concrete evidence and it is not possible to obtain evidence by other means during the prosecution performed for a crime, the high criminal court or, in case of peril in delay, the public prosecutor, may decide to listen, record, and utilize the signal data of the communication of the suspect or the accused. The public prosecutor shall submit his decision immediately to the approval of the court and the court shall decide within twenty-four hours. In case of expiration of the duration or the court decides otherwise, the measure shall be removed immediately by the public prosecutor. The measures to be taken in accordance with this paragraph shall be decided unanimously by the high criminal court. Unanimous decision is also required for making this decision upon objection.

(2) (**Additional: 21/2/2014- 6526/Article 12.)** If the owner of the line or means of communication, on which a decision of measure is to be made in accordance with this article is known, a document or report that shows the identity of such owner shall be attached while making the request.

(3) The communication between the suspect or the accused and the persons who may refrain from testimony shall not be recorded. If this circumstance is revealed after the record is taken, the relevant record shall be deleted immediately.

(4) The decision that is made in accordance with the paragraph 1 shall include the nature of the charged crime, the identity of the person who will be subject to the measure, type of the means of communication, telephone number or code that has enabled location of the connection of the communication, and the type, scope and duration of the measure. The duration of the measure shall not exceed two months, and this period may be extended by a month. **(Additional provision: 25/5/2005-5353/Article 17)** However, for crimes committed within the activities of a criminal organization, the court may decide to extend the duration several times, each time for no longer than one month and no longer than three months in total.

(5) In order to apprehend the suspect or the accused, the location of the mobile phone may be identified upon the decision of the judge, or in case of peril in delay, upon the decision of the public prosecutor. The decision made in this regard shall include the mobile telephone number and the duration of the identification. The duration of the identification shall not exceed two months, and this period may be extended by a month.

(6) (**Additional**: **2/12/2014-6572/Article 42)** Identification of the communication of the suspect or the accused by means of telecommunication shall be based on the decision of the judge at the stage of investigation and on the court decision at the stage of prosecution. The decision shall include the nature of the charged crime, the identity of the person who will be subject to the measure, type of the means of communication, telephone number or code that has enabled location of the connection of the communication, and duration of the measure.

(7) Decisions make and procedure conducted according to the provisions of this article shall be kept confidential while the measure is pending.

(8) The provisions in this article with regard to recording and utilizing the signal data only be applicable for the crimes specified below:

a) The following crimes in the Turkish Penal Code;

1. Migrant smuggling and human trafficking (articles 79, 80),
2. Intentional killing (articles 81, 82, 83),
3. Torture (articles, 94, 95),
4. Sexual assault (except the first paragraph, article 102),
5. Child sexual abuse (article 103),
6. **(Additional: 21/2/2014 – 6526/Article 12)** Qualified theft (article 142) and robbery (article 148, 149),
7. Production and trade of narcotics and psychotropic substances (article 188),
8. Counterfeiting money (article 197),
9. (Repealed: 21/2/2014 – 6526/Article 12)
10. Prostitution (article 227),
11. Fraud during a tender (article 235),

12. Bribery (article 252),
13. Laundering of assets acquired by an offence (article 282),
14. (**Amended: 2/12/2014-6572/Article 42)** Disrupting the unity and integrity of the state (article 302),
15. (**Additional**: **2/12/2014-6572/Article 42)** Offences against the constitutional order and its functioning (articles 309, 311, 312, 313, 314, 315, 316),
16. Offences against the secrets of the state, and espionage (articles 328, 329, 330, 331, 333, 334, 335, 336, 337).
(b) Arms trafficking crimes (article 12) defined in the Law for Firearms, Knives and Other Tools.
c) (**Additional**: **25/5/2005-5353/Article 17)** The crime of embezzlement as defined the paragraphs (3) and (4) of the article 22 of the Banking Act,
d) Crimes defined in the Law on Combating Smuggling, which require imprisonment.
e) Crimes defined in the articles 68 and 74 of the Law on Protection of Cultural and Natural Property.
(9) No one may listen and record the communication of another person by means of telecommunication except under the principles and procedures determined in this article.

Interception of content data
Code No. 5271 on Criminal Procedure
Location, listening and recording of communication
Article 135 – (1) **(Amended: 21/2/2014 - 6526/Article 12)** Where there are strong reasons for suspicion based on concrete evidence and it is not possible to obtain evidence by other means during the prosecution performed for a crime, the high criminal court or, in case of peril in delay, the public prosecutor, may decide to listen, record, and utilize the signal data of the communication of the suspect or the accused. The public prosecutor shall submit his decision immediately to the approval of the court and the court shall decide within twenty-four hours. In case of expiration of the duration or the court decides otherwise, the measure shall be removed immediately by the public prosecutor. The measures to be taken in accordance with this paragraph shall be decided unanimously by the high criminal court. Unanimous decision is also required for making this decision upon objection.
(2) (**Additional: 21/2/2014- 6526/Article 12.)** If the owner of the line or means of communication, on which a decision of measure is to be made in accordance with this article is known, a document or report that shows the identity of such owner shall be attached while making the request.
(3) The communication between the suspect or the accused and the persons who may refrain from testimony shall not be recorded. If this circumstance is revealed after the record is taken, the relevant record shall be deleted immediately.
(4) The decision that is made in accordance with the paragraph 1 shall include the nature of the charged crime, the identity of the person who will be subject to the measure, type of the means of communication, telephone number or code that has enabled location of the connection of the communication, and the type, scope and duration of the measure. The duration of the measure shall not exceed two months, and this period may be extended by a month. **(Additional provision: 25/5/2005-5353/Article 17)** However, for crimes committed within the activities of a criminal organization, the court may decide to extend the duration several times, each time for no longer than one month and no longer than three months in total.
(5) In order to apprehend the suspect or the accused, the location of the mobile phone may be identified upon the decision of the judge, or in case of peril in delay, upon the decision of the public prosecutor. The decision made in this regard shall include the mobile telephone number and the duration of the identification. The duration of the identification shall not exceed two months, and this period may be extended by a month.
(6) (**Additional**: **2/12/2014-6572/Article 42)** Identification of the communication of the suspect or the accused by means of telecommunication shall be based on the decision of the judge at the stage of investigation and on the court decision at the stage of prosecution. The decision shall include the nature of the charged crime, the identity of the person who will be subject to the measure, type of the means of communication, telephone number or code that has enabled location of the connection of the communication, and duration of the measure.
(7) Decisions made and procedure conducted according to the provisions of this article shall be kept confidential while the measure is pending.
(8) The provisions in this article with regard to recording and utilizing the signal data only be applicable for the crimes specified below:
a) The following crimes in the Turkish Penal Code;
1. Migrant smuggling and human trafficking (articles 79, 80),
2. Intentional killing (articles 81, 82, 83),
3. Torture (articles, 94, 95),
4. Sexual assault (except the first paragraph, article 102),
5. Child sexual abuse (article 103),
6. **(Additional: 21/2/2014 – 6526/Article 12)** Qualified theft (article 142) and robbery (article 148, 149),
7. Production and trade of narcotics and psychotropic substances (article 188),
8. Counterfeiting money (article 197),
9. (Repealed: 21/2/2014 – 6526/Article 12)
10. Prostitution (article 227),
11. Fraud during a tender (article 235),
12. Bribery (article 252),
13. Laundering of assets acquired by an offence (article 282),
14. (**Amended: 2/12/2014-6572/Article 42)** Disrupting the unity and integrity of the state (article 302),
15. (**Additional**: **2/12/2014-6572/Article 42)** Offences against the constitutional order and its functioning (articles 309, 311, 312, 313, 314, 315, 316),
16. Offences against the secrets of the state, and espionage (articles 328, 329, 330, 331, 333, 334, 335, 336, 337).
(b) Arms trafficking crimes (article 12) defined in the Law for Firearms, Knives and Other Tools.
c) (**Additional**: **25/5/2005-5353/Article 17)** The crime of embezzlement as defined the paragraphs (3) and (4) of the article 22 of the Banking Act,

d) Crimes defined in the Law on Combating Smuggling, which require imprisonment.
e) Crimes defined in the articles 68 and 74 of the Law on Protection of Cultural and Natural Property.
(9) No one may listen and record the communication of another person by means of telecommunication except under the principles and procedures determined in this article.

Corresponding article in the legislation:
Turkish Penal Code no. 5237, Articles 8,9,10,11,12,13
Territorial jurisdiction
Article 8- (1) Turkish law shall apply to all criminal offences committed in Turkey. If the act is partially or fully committed in Turkey or its consequence occurs in Turkey, the offence is considered to be committed in Turkey.
(2) If the criminal offence is committed;
a) within Turkish territory, airspace or in Turkish territorial waters,
b) on the open sea or in the space extending directly above these waters and in, or by using, Turkish sea and air vessels,
c) in, or by using, Turkish military sea or air vehicles,
d) on or against a fixed platform erected on the continental or in the economic zone of Turkey, the offence is considered to have been committed in Turkey.
Conviction in a foreign country
Article 9- (1) Any person who is convicted in a foreign country for an offence committed in Turkey shall be subject to retrial in Turkey.
Offences related to a duty
Article 10- (1) Where a person employed as a public officer or assigned a duty in Turkey and commits an offence related to such office or duty shall be subject to retrial in Turkey even if he is convicted in a foreign country.
Offences committed by citizens
Article 11- (1) If a Turkish citizen commits in a foreign country a crime other than those specified in the 13, which is punishable by an imprisonment of at least one year under Turkish laws, and if the said offender is in Turkey, he shall be punished under Turkish law provided that no conviction is made in the foreign country and prosecution is possible in Turkey.
(2) Where the offence is punishable by imprisonment with a lower limit less than one year, trial depends on a complaint filed by the victim or the foreign government. In such cases, the complaint must be filed within six months following the entry of the citizen into Turkey.
Offences committed by foreigners
Article 12- (1) If a foreigner commits in a foreign country a crime to the detriment of Turkey other than those specified in the 13, which is punishable by an imprisonment of at least one year under Turkish laws, and if the said offender is in Turkey, he shall be punished under Turkish laws. Trial is subject to the request by the Minister of Justice.
(2) Where the aforementioned offence is committed to the detriment of a Turkish citizen or to the detriment of a legal entity established under Turkish civil law and the offender is present in Turkey, and there has been no conviction in a foreign country for the same offence, upon the making of a complaint by the victim, he shall be subject to penalty under Turkish law.
If the victim is a foreigner, the offender shall be subject to criminal proceedings, upon the request of the Minister of Justice, provided the following conditions are fulfilled:
a) The offence is punishable by imprisonment of at least three years under Turkish laws.
b) There is not an extradition agreement in force, or the extradition request is not accepted by the government of the country where the offence was committed or the country of the perpetrator's nationality.
(4) A foreign national who is convicted by a foreign court for an offence described in the first paragraph or who acquits or whose case was dismissed or has lost its prosecutable status for any reason shall be subject to another trial in Turkey.
Other offences
Article 13- (1) Where the following offences are committed by a citizen or a non-citizen of Turkey in a foreign country, Turkish laws shall be applicable:
a) The offences described under Volume II, Chapter 1.
b) The offences described under Volume II, Chapter 4, Part 3, 4, 5, 6, 7, and 8.
c) Torture (articles, 94, 95).
d) Intentional pollution of the environment (Article 181).
e) Production and trade of narcotics or psychotropic substances (Article 188), facilitating the use of narcotics or psychotropic substances (Article 190).
f) Counterfeiting money (Article 197), manufacturing and trading of instruments used in the production of money and valuable seals (Article 200); counterfeiting a seal (Article 202).
g) Prostitution (article 227).
h) (Repealed: 26/6/2009 – 5918/Article 1)
Seizing control or hijacking of air, sea or rail transport vehicles (Article 223, paragraphs 2 and 3) and offences related to the damaging of such vehicles (Article 152).
(2) (Additional paragraph 2: 29/6/2005 – 5377/Article 3) Except for the offences described under Volume II, Chapter 4, Parts 3, 4, 5, 6, and 7, conducting criminal proceedings in Turkey for crimes within the scope of paragraph one shall be subject to a request of the Minister of Justice.
(3) Even where a conviction or acquittal pursuant to the offences listed in paragraph 1, subparagraphs (a) and (b) have occurred in a foreign country, trial shall be conducted in Turkey upon the request of the Ministry of Justice.
The law is mentioned according to [88]

Voyeurism
Turkish Penal Code
Privacy of private life
Article 134 - (1) Any person who violates the privacy of persons shall be sentenced to imprisonment or judicial fine from six months to two years. In the event of violation of confidentiality by recording images or sounds, the lower limit of the sentence shall not be less than one year.

(2) Anyone who exposes images or sounds related to the private life of a person shall be sentenced to imprisonment of one to three years. If the act is committed through the press and publication, the penalty is increased by half.

C. Organizations against Cybercrime in Turkey

Top Level Cyber Security Organisation Structure in Turkey [55]

National Cyber Security Board (Ulusal Siber Güvenlik Kurulu)

The Board is responsible for approving the plans, programmes, reports, procedures, principles, and standards prepared by the governmental bodies that are represented on the board and ensuring their implementation and coordination, to determine the measures to be taken by public institutions and organisations and natural and legal persons in relation to national cyber security. The Cyber Security Board is the top governmental organisation regarding the governance of national cyber security. The level of representation of the ministries and public institutions and organisations involved in the National Cyber Security Board and its members is determined by the Ministerial Cabinet [55].

The Board's responsibilities are;

- To approve policies, strategies and action plans related to cyber security and to make the necessary decisions for effective implementation of it throughout the country
- To bid on proposals for the identification of critical infrastructures
- To determine the institutions and organisations to be exempted from all or some of the provisions related to cyber security
- To perform other duties given by law [55]

National CERT (USOM - Ulusal Siber Olaylara Müdahale Merkezi)

USOM was established under BTK (Bilgi Teknolojileri ve İletişim Kurumu), the Information and Communication Technologies Authority, and constantly monitors and provides warnings and announcements for cyber security incidents. It also establishes national and international coordination for the prevention of cyber-attacks against critical sectors. Additionally, to assist the organisations responsible for forming their own sub-CERTs (SOME), Guidelines for Establishing and Management of Institutional CERTs was released [63].

Cyber Events Response Team (SOME – Siber Olaylara Müdahele Ekibi)

In order to ensure cyber security structuring in Turkey, studies involving technical and legal sanctions have been made. As a result of these efforts, "Decision on the Execution and Coordination of National Cyber Security Studies" was published in the "Official Gazette" on 20 October 2012 with the decision of the Council of Ministers. According to the decision, the "Cyber Security Council" was established to approve the procedures, principles and standards in the field of cyber security and to ensure their implementation and coordination. As a result of the meeting held by the Cyber Security Council, the action plan published by the Ministry of Transport, Maritime Affair, and Communications was adopted. In this context, National CERT (USOM), whose main task is coordination and cooperation, has been established and started its activities. In addition, the guideline has been designated as Institutional SOME and Sectoral SOME. These organisations are prepared for the benefit of institutions that are obliged to establish Institutional SOME within the scope of the Communiqué on Procedures and Principles of Establishment, Duties and Works of Cyber Events Response Teams published in the Official Gazette was dated 11 November 2013 and numbered 28818 [56].

Cyber Events Response Team involves the following agencies and organisations:

- Institutional Cyber Events Response Team
- Sectoral Cyber Events Response Team [56]

SOME's responsibilities are;

- Classification and Protection of Information
- Systems for holding data
- Protection for destruction of data
- Distribution and access of information
- Use of systems that are related to SOME-based technology [56]

The Presidency of Defence Industries (SSB – Savunma Sanayi Bakanlığı)

The cyber defence industry is considered a part of the national defence industry, thus the defence projects in the cyber domain are overseen and contracted by SSB with respect to the requirements and strategic plan of Turkish Armed Forces and national security [55].

The Ministry of Transport and Infrastructure (Ulaştırma ve Altyapı Bakanlığı)

By Cabinet decision of October 2012 on implementing, administering and coordinating national cyber security

actions, the preparation and coordination of policy, strategy and action plans regarding the governance of national cyber security were given to The Ministry of Transport and Infrastructure, which acts as the responsible governmental agency and oversees all other cyber security entities through the state [55].

The Scientific and Technological Research Council of Turkey's (TÜBİTAK – Türkiye Bilimsel ve Teknolojik Araştırma Kurumu)

The activities of Cyber Security Institute (CSI) which was firstly established as the IT Systems Security Division under the National Electronics and Cryptology Research Institute, was aimed at the improvement of the national cyber security capacity in 1997. It has been working as a distinct institution under TÜBTAK BBLGEM since 2012. The Cyber Security Institute offers government, personal and army organisations with data technologies and safety consultant facilities and performs exploration and advancement operations. The Cyber Security Institute has led through its many good initiatives to the growth of IT safety know-how [57].

The Turkish National Police (Türkiye İçişleri Bakanlığı Emniyet Genel Müdürlüğü)

Department of Cyber Crime Prevention provides support for the investigation of crimes committed using information technology and examines and manages digital evidence to ensure that the dispersed structure of provincial law enforcement units does not have any negative effects. It gathers forensic data under a single roof to prevent duplicating investment and to fight cybercrime effectively and efficiently. The Department of Cyber Crime Prevention was established within the Turkish National Police General Directorate (EGM) by a Cabinet Decision of 2011 [55].

The Turkish Armed Forces (TSK – Türkiye Silahlı Kuvvetleri)

The Turkish Armed Force (TSK) runs their cyber security and cyber defense policies and strategy according to existing national, international and NATO standards. Maintaining a continuous synchronization with the Ministry of Transport and Infrastructure as the top national cyber security authority and with the National CERT (USOM) are held as top priorities, enabling the TSK to stay up to date with current developments in terms of cyber threats, attacks and technology, and to avoid duplication of effort. Turkish military cyber security policies and measures are outlined by regulations issued by the Turkish General Staff, which follows Cabinet's national cyber security decisions and related laws.

In keeping up with the continuous evolution of cyber security and cyber defense, especially in the last 20 years, the Turkish Armed Forces perceive cyber defense as a distinct military domain, correlating to NATO's recognition of cyberspace as a domain of operations in the July 2016 Warsaw Summit. To cope with the increasing threats and hostility in cyberspace, whether from state or non-state actors, establishing and maintaining strong and resilient cyber defense posture and capabilities are among the top priorities of Turkey's defense strategy [55].

The National Intelligence Agency (MIT - Milli İstihbarat Teşkilatı)

In Turkey, the National Intelligence Service (MIT) is one of the units responsible for collecting the necessary intelligence to prevent cyber security threats. The "Law Amending the Law on State Intelligence Services and the National Intelligence Agency" (Law No. 6532, Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanununda Değişiklik Yapılmasına Dair Kanun), which gave MIT mandate on this area, entered into force on April 26, 2014. In the new law, the responsibility of MIT is redefined as:

"To deliver the produced intelligence to relevant institutions on Foreign Intelligence, National Defense, Counter-terrorism, international crimes and cyber security topics by using all types of technical intelligence, human intelligence via utilizing relevant tools, methods and systems with the process of collecting, recording and analyzing pertinent information, document, news and data." [54].

D. International Cooperation

All laws are mentioned according to website of Council of Europe [58]

Extradition

Law no. 6706 on International Judicial Cooperation in Criminal Matters

Extradition from Turkey to a foreign state

ARTICLE 10 - (1) A foreigner who is being investigated or prosecuted or convicted with imprisonment by judicial authorities due to a crime that is committed in a foreign country may be extradited to the requesting country for conclusion of the investigation or prosecution or execution of the penalty.

(2) Requests for extradition may be accepted for the crimes restricting freedom for a maximum period of one year or more during the investigation or prosecution under the law of the requesting state or Turkey. The penalty that is imposed must be restricting freedom for at least four months in order for the request of extradition to be accepted with regard to finalized imprisonment decisions. If the person requested for

extradition has committed multiple offences, the terms of imprisonment may be added up for extradition even if some the term of imprisonment for some of such offences are below the specified periods.
(3) If multiple requests from different states for extradition are made for the same person, the Central Authority shall decide which request to prioritize based on the severity and location of offences, reception order of requests, citizenship of the offender, and the possibility of re-extradition.
(4) In the event of extradition, a person may be subject to trial or the penalty convicted to the person may be executed for the crimes that make the basis of the decision of extradition only.

Rejection of extradition request
ARTICLE 11 - (1) The request for extradition shall not be accepted if:
a) the person requested for extradition is a Turkish citizen except for the liabilities brought by being a party to the International Criminal Court.
b) there is strong suspicion that the person requested for extradition would be subject to an investigation or prosecution, punished or subject to torture or maltreatment due to his race, ethnic origins, religion, citizenship, membership of a social group.
c) the act that makes the basis of the request for extradition is;
1) a thought crime, political crime or a crime related to a political crime,
2) merely a military crime,
3) committed against the security of the Turkish State, or to the detriment of a Turkish citizen or a legal entity that was established under Turkish laws,
4) a crime that is in the jurisdiction of Turkey,
5) subject to time limitation or pardoned.
ç) a former decision of acquittal or imprisonment was made in Turkey for the act subject to the request with regard to the person requested for extradition.
d) the request for extradition is for crimes that are punishable by death or a penalty that does not comply with human dignity.
(2) When all characteristics, particularly the way of commission, the means by which the crime is committed, and the severity of the consequences are considered for an act that makes the basis for the extradition request in the item (1) of the subparagraph (c) of the first paragraph, the relevant act may not be accepted as a political crime. Genocide and crimes against humanity shall not be considered political crimes.
(3) If there are grounds for rejection with regard to the nature of the crime in the item (d) of the first paragraph, the extradition request may be accepted if sufficient guarantee is given by the requesting state for non-execution of the predicted penalty.
(4) The request for extradition may not be accepted for personal reasons such as the requested person is younger than eighteen years as of the date of the request, lives in Turkey for a long time or is married, which would cause the said person or his family suffer disproportionately to the severity of the act.

The relationship between extradition and deportation
ARTICLE 12 - (1) A foreigner shall not be deported without taking the opinion of the Central Authority at the extradition process.
(2) A foreigner shall not be deported to a country, extradition request of which is declined, without taking the opinion of the Central Authority.

Examination by the Central Authority
ARTICLE 13 - (1) The Central Authority shall examine the extradition requests, and may request additional information and documents if it considers necessary, and it declines the requests that do not fulfill necessary conditions.
(2) The requests that fulfill necessary conditions shall be submitted to the public prosecutor affiliated with the competent high criminal court.

Provisional arrest
ARTICLE 14 - (1) In case of serious suspicion that a crime that is specified in the extradition request is committed, the offender may be put under provisional arrest before the extradition request is received by the Central Authority upon the request of the relevant state and approval of the Central Authority within the framework of the provisions of international treaties signed by Turkey and the principle of reciprocity.
(2) A person with a strong suspicion of having committed a crime that is described under the article 12, paragraph 3, subparagraph (a) of Turkish Penal Code no. 5237 dated 26/9/2004 and who may be subject to extradition request, may be arrested temporarily without the request of the relevant state.
(3) The temporary request for arrest by the relevant state shall be submitted to the Ministry of the Interior by the Central Authority for apprehending the offender and sending him to the public prosecutor's office. The apprehended person shall be referred to the justice of the peace for a decision of arrest within twenty-four hours. The justice of the peace shall decide on the request after he informs the person requested to be arrested about the possibility of consented extradition and its legal consequences.
(4) The duration of temporary arrest shall be governed by the provisions of relevant international treaties. Temporary arrest shall not exceed forty days within the framework of the principle of reciprocity.
(5) A decision of judicial control may be made in a manner that prevents the offender from escaping instead of temporary arrest in accordance with the article 109 of the Law on Criminal Procedure.
(6) If the relevant state fails to submit extradition documents within the period specified in the fourth paragraph, the decision of temporary arrest or judicial control shall be revoked. This shall not hinder implementation of protective

measures for the purpose of extradition after the request for extradition is received.

Duties and powers

ARTICLE 15 - (1) The high criminal court of the place where the offender is located shall have jurisdiction for deciding for the extradition request. If the location of the offender is not clear, Ankara high criminal court shall have jurisdiction.

(2) The public prosecutor shall request the high criminal court to decide on the extradition request.

Implementation of protective measures for the purpose of extradition

ARTICLE 16 - (1) The high criminal court may decide on the protective measures for the person requested for extradition, in accordance with the provisions of the Law on Criminal Procedure.

(2) If the person is arrested during the period of extradition, the detention until the extradition shall be examined by the high criminal court every thirty days the latest.

(3) If a decision of extradition is not made within a year in accordance with the article 19 following the finalization of the decision on the acceptance of extradition request by the high criminal court, the protective measures on the offender shall be removed.

(4) The total period of detention shall not exceed the period of execution of the penalty that may be imposed for the offence or the conviction.

Procedure of consented extradition

ARTICLE 17 - (1) If a person consents to extradition, he may be extradited to the requesting state without implementation of the regular extradition procedure.

(2) The high criminal court shall inform the person about his rights under the Law on Criminal Procedure, and the nature and legal consequences of the consented extradition. The person is asked whether he accepts the procedure of consented extradition.

(3) Once the person has accepted the procedure of consented extradition, the court shall decide whether the extradition request is acceptable based on the provisions of this Law and international treaties signed by Turkey. This decision may be objected. When the decision is finalized, extradition documents shall be submitted to the Central Authority.

(4) Execution of the decision of extradition by consented extradition procedure shall be subject to the approval of the Central Authority.

Extradition hearing

ARTICLE 18 - (1) If the person does not accept the procedure of consented extradition, the court shall decide whether the extradition request is acceptable based on its examination of the terms of extradition in accordance with the provisions of this Law and international treaties signed by Turkey.

(2) If the documents submitted by the requesting state are not considered sufficient, the court may request submission of additional information and documents within an appropriate period.

(3) No request for participation shall be made in extradition hearings.

(4) Court decision can be appealed. The Court of Cassation shall conclude such applications within three months. When the decision is finalized, extradition documents shall be submitted to the Central Authority with the decision.

Decision of extradition

ARTICLE 19 - (1) If the high criminal court decides that the extradition request is acceptable, execution of this decision shall be subject to the proposal of the Minister of Justice and approval of the Prime Minister with the opinions of the Ministry of Foreign Affairs and the Ministry of Internal Affairs taken.

(2) The Central Authority shall expressly notify the requesting state and the person requested to be extradited whether the request is accepted or rejected.

Surrender

ARTICLE 20 - (1) Surrender processes of a person who is decided to be extradited shall be conducted in cooperation with the relevant ministries.

(2) If the person decided to be extradited is not received on the date agreed with the authorities of the requesting state for no justifiable reason, the court shall revoke the protective measures on this person within thirty days from the date mentioned above.

(3) If the person that is decided to be extradited is subject to a conviction that requires investigation or prosecution, or execution in Turkey for another offence, or if he is not fit for travel, the Central Authority may decide to postpone the surrender. This decision shall be notified to the relevant person and the requesting state.

(4) Any items that are considered useful as evidence or obtained by committing the crime and seized when the person is apprehended or that appeared later may be surrendered to the requesting state. If the person requested for extradition dies, escapes or a decision cannot be made for similar reasons, the abovementioned items may still be surrendered.

(5) Surrender of the items may be postponed when it is required for an investigation or prosecution in progress in Turkey.

(6) Requests for surrendering the items that belong to third persons in good faith shall not be fulfilled.

Transit proceedings

ARTICLE 21 - (1) Where a person is being extradited from a state to another state, transit of that person through Turkey may be permitted if the terms of extradition are permissible under Turkish law.

(2) The request of transit shall be evaluated by the Central Authority, and the decision made shall be notified to the competent authority of the requesting state.

(3) If the transit takes longer than twenty-four hours and there arises the need to restrict the freedom of the person for this reason, the justice of the peace may issue a decision of temporary detention in order to facilitate transit, provided that it does not exceed seven days.
(4) Where there are circumstances that require rejection of the transit or the person commits an offence that requires *ex-officio* investigation during the transit, the transit may be stopped.
(5) For the transfer of convicts from a country to another, the provisions of this article shall be applicable for transits through Turkey.

Requests and conditions of Turkey regarding extradition
ARTICLE 22 - (1) Judicial authorities may request extradition of a person in a foreign country, who is ordered to be apprehended or decided to be arrested, to Turkey for conclusion of investigation or prosecution, or execution of imprisonment decisions.
(2) Extradition of a person may be requested for an offence that requires imprisonment with the upper limit of one year or more. In order to request extradition for finalized conviction of imprisonment, the term of the imprisonment must be at least four months. If the person requested for extradition has committed multiple offences, the terms of imprisonment may be added up for extradition even if some the term of imprisonment for some of such offences are below the specified periods.
(3) The request shall be submitted to the foreign state if approved by the Central Authority. However, the Central Authority may decline the extradition request without submitting it to the foreign state if:
a) The request does not fulfill the conditions required for extradition.
b) Requesting extradition causes an express inconsistency between the individual good and public good when the term in penal institutions is taken into consideration.
c) The national security or international relations of Turkey are likely to be damaged.
(4) The provisions in the articles 20 and 21 shall be applicable as appropriate for extradition of a person to Turkey through third countries.

General principles relating to mutual assistance
Law no. 6706 on International Judicial Cooperation in Criminal Matters
Judicial cooperation by means of audiovisual communication
ARTICLE 9 - (1) Audiovisual communication techniques may be asked to be used in fulfilling the judicial cooperation request. Such processes shall be performed under the control of the authorities of the performing state and in accordance with the laws of such state.
(2) If Turkish judicial authorities request judicial cooperation to be made by means of audiovisual communication, this shall be performed under the control of Turkish judicial authorities and in accordance with Turkish laws, provided that they are provided for in international treaties.
(3) If a foreign state request judicial cooperation to be made by means of audiovisual communication, this shall be performed under the control of the requesting state's judicial authorities and in accordance with the laws of the requesting country, provided that they are provided for in international treaties. Turkish judicial authorities shall attend this process to observe that the fundamental principles of Turkish law are not violated

Expedited preservation of stored computer data
Law no. 6706 on International Judicial Cooperation in Criminal Matters
The requests of Turkish judicial authorities
ARTICLE 7 - (1) Judicial authorities may request judicial cooperation in conclusion of investigation or prosecution, or for the matters that may be needed for executing the decisions on imprisonment. In such cases, the following provisions shall be applicable:
a) Temporary measures may be requested for protecting the evidence before the judicial cooperation request if delays are considered detrimental.
b) Warnings related to implementation of restrictive or coercive measures shall not be included in judicial cooperation requests related to notifications.
c) A request may be made for attendance during the performance of the action that is referred to in the request for judicial cooperation.
ç) The processes performed by the relevant state under the judicial cooperation request shall be considered valid under Turkish law.
(2) If, within the scope of an investigation or prosecution, any information that may cause another state to start criminal investigations are learned by judicial authorities, such information may be notified to the Central Authority for submission to the relevant state without request.

The requests of foreign judicial authorities
ARTICLE 8 - (1) The following provisions shall be applicable to judicial cooperation requests:
a) The requests shall be fulfilled in compliance with Turkish law. If a special procedure is requested, the request shall be fulfilled in accordance with this request provided that it is not in contradiction with Turkish law.
b) Turkish judicial authorities may decline requests partially or fully or request additional information or documents when considered necessary.
c) Temporary measures may be taken for protecting the evidence before the judicial cooperation request is sent if delays are considered detrimental. If the judicial cooperation request is not received by the Central Authority within forty days following the date of the temporary measure, it shall be revoked immediately by the relevant authorities.
d) If search or seizure is requested, the offence for which the request is made must be suitable for extradition. Regarding the value of the property, rights and receivables that are

seized upon request, Turkish judicial authorities shall request information from the requesting state at least once a year to see whether the measure is to be continued.

e) If a judicial cooperation request related to notifications includes a warning related to implementation of restrictive or coercive measures, the request shall be declined.
f) Foreign judicial authorities may request to attend before Turkish judicial authorities while the action subject to the request for judicial cooperation is executed. The request shall be fulfilled if it is approved.
g) If a decision of conviction or approval is made for the person by Turkish courts, or if the offence is pardoned or subject to time limitation, judicial cooperation requests for the same act may not be fulfilled.

Trans-border access to stored computer data with consent or where publicly available
Law no. 6706 on International Judicial Cooperation in Criminal Matters
Judicial cooperation by means of audiovisual communication
ARTICLE 9 - (1) Audiovisual communication techniques may be asked to be used in fulfilling the judicial cooperation request. Such processes shall be performed under the control of the authorities of the performing state and in accordance with the laws of such state.
(2) If Turkish judicial authorities request judicial cooperation to be made by means of audiovisual communication, this shall be performed under the control of Turkish judicial authorities and in accordance with Turkish laws, provided that they are provided for in international treaties.
(3) If a foreign state request judicial cooperation to be made by means of audiovisual communication, this shall be performed under the control of the requesting state's judicial authorities and in accordance with the laws of the requesting country, provided that they are provided for in international treaties. Turkish judicial authorities shall attend this process to observe that the fundamental principles of Turkish law are not violated.

E. Cyber Crime Trainings and Tools in Turkey

All trainings and tools are mentioned in the document of The Council of Europe and The European Union [61]

It is essential that each role attract the appropriate level of training and education to enable to be effective and to interact with other cybercrime investigation functions both nationally and internationally.

The stakeholders and their learning requirements identified as relevant to the Turkish National Police are:

First responders

- Legal codes CMK134, Arama ve El Koyma Yönetmeliği (Search and Seizure Regulation)
- Types of court orders
- Modus operandi of cyber crime types
- Evidence: integrity and stability
- Data storage capacity of electronic devices
- Computer and systems basics
- Live system analysis tools
- Data imaging tools (Hardware and Software)
- Requirements of evidence storage devices
- Anti-forensics techniques
- Investigation description and preparation
- Security of crime scene
- Crime scene interviews
- Running systems response techniques
- Static computer system response techniques
- Rechargeable mobile device Response
- Labelling, packaging and Transport

Cybercrimes investigators

- Legal codes CMK 134, TCK 142/2-e, 58/1-f, 243, 244, 245 Arama ve El Koyma Yönetmeliği (Search and Seizure Regulation)
- Awareness in cyber crimes
- Modus operandi of cyber crimes
- Internet architecture
- Information gathering techniques
- Basic Internet investigation techniques
- Command line interpreter
- Network live investigation techniques
- IRC, P2P investigations techniques
- Server response analysis
- Crime analysis
- Report writing
- Computer forensics for investigators
- Skimming investigation techniques
- Carding investigation techniques
- Phishing, Vishing, Smishing investigation techniques
- Covert investigation techniques
- Wireless investigation technique

Computer forensics examiners

- Basic computer forensics (Partition - Format, File Signatures, Deleted Files, System Shutdown)
- Operating systems (Linux, Mac, Windows)
- File Systems - Fat, Ntfs, Mac, Linux
- Working principles of data storage (CD/DVD, HDD, BluRay, Flash, MMC etc.)
- Database basics
- Network forensics (Silent Runner, Prodiscover network etc.)

- Malware analysis
- Steganography
- Live data forensics
- EnCase
- FTK
- Xways
- Data Recovery Tools - Software/Hardware (PC3000, DataCompass, HDDoctor, FlashDoctor etc.)

Decrypters

- Basic computer forensics (Partition - Format, File Signatures, Deleted Files, System Shutdown)
- Operating systems (Linux, Mac, Windows)
- File Systems - Fat, Ntfs, Mac, Linux
- Working principles of data storage (CD/DVD, HDD, BluRay, Flash, MMC etc.)
- Database basics
- Network forensics (Silent Runner, Prodiscover network etc.)
- Malware analysis
- Steganography
- Live data forensics
- Password Recovery Tools (PRTK, Passware etc.)

Mobile examiners

- Basic computer forensics (Partition - Format, File Signatures, Deleted Files, System Shutdown)
- Operating systems (Linux, Mac, Windows)
- File Systems - Fat, Ntfs, Mac, Linux
- Working principles of data storage (CD/DVD, HDD, BluRay, Flash, MMC etc.)
- Database basics
- Network forensics (Silent Runner, Prodiscover network etc.)
- Malware analysis
- Mobile Forensics Tools (CelleBrite, Paraben, XRY, Tarantula etc.)

Data carvers

- Basic computer forensics (Partition - Format, File Signatures, Deleted Files, System Shutdown)
- Operating systems (Linux, Mac, Windows)
- File Systems - Fat, Ntfs, Mac, Linux
- Working principles of data storage (CD/DVD, HDD, BluRay, Flash, MMC etc.)
- Database basics
- Network forensics (Silent Runner, Prodiscover network etc.)
- Malware analysis
- EnCase
- FTK
- Xways
- Payment systems (MSR, skimmer, ATM)
- Password Recovery Tools (PRTK, Passware etc.)
- Data Recovery Tools - Software/Hardware (PC3000, DataCompass, HDDoctor, FlashDoctor etc.)

Analysts

- Awareness in cyber crimes
- Modus operandi of cyber crimes
- Internet architecture
- Basic Internet investigation techniques
- Computer forensics for investigators
- Crime analysis 4 x 4
- Information gathering techniques
- Database programming
- Crime analysis tools
- Visualization of analysis reports

Cybercrimes trainers

- Trainer development course
- Training management
- Internet investigator course
- Analyst course
- Basic computer forensics course
- Awareness in cyber crimes
- Modus operandi of cyber crimes
- Internet architecture
- Basic Internet investigation techniques
- Training field topics

Senior staff

- Legal Code CMK 134, TCK 142/2-e, 58/1-f, 243, 244, 245
- Arama ve El Koyma Yönetmeliği (Search and Seizure Regulation)
- Modus Operandi of Cyber Crime Types
- Evidence: Integrity and Stability
- Data Storing Capacity Electronic Devices
- Computer Forensics for Investigators
- Cyber Crime Personnel Management
- Awareness in Cyber Crimes
- Modus Operandi of Cyber Crimes
- Internet Architecture
- Basic Internet Investigation Techniques

Very senior managers

- Cyber Crime Trends
- Cyber Crimes Modus Operandi Examples
- Awareness in Cyber Crimes

Industry and academia awareness training

- Cyber Crime Trends
- Cyber Crimes Modus Operandi Examples
- Awareness in Cyber Crimes
- Cooperation Possibilities

Police investigators

- Modus Operandi of Cyber Crime Types
- Evidence: Integrity and Stability
- Data Storing Capacity Electronic Devices
- Computer Forensics for Investigators
- Information Gathering Techniques

All police personnel

- All police officers at Police School or Police Academy need to receive basics of cybercrime investigators and volatile digital evidence before they join Turkish National Police.
- Modus Operandi of Cyber Crime Types
- Evidence: Integrity and Stability
- Data Storing Capacity Electronic Devices

The Turkish Gendarmerie also has a group of staff that need to be catered for in their strategy. These are identified along with the learning requirements as follows:

First Responders

(Introductory training on the following subjects)
- Electronic evidence related devices, hardware etc.
- Network related hardware (modem, switch, WAP etc.)
- Tools/devices for imaging
- How to secure a crime scene
- Officer health and safety
- How to seize electronic evidence
- Operating systems
- Mobile phones

(Advanced knowledge needed in addition to the above)
- Computer related hardware in detail
- RAID types (either software/hardware)
- Database systems
- Live forensics
- Operating systems Windows/Linux/Unix
- Encryption methods/programs/hardware
- Servers (how to deal with)
- Anti-forensic techniques

Cybercrime Investigator/specialists
- Internet structure in detail
- How it works in detail?
- All internet protocols
- Internet activity monitoring and analyzing
- File sharing technologies (P2P applications)
- Video technologies
- Social engineering

Digital Forensic Examiners/specialists
- Digital forensics tools (software, hardware)
- Open source DF tools
- Imaging
- Operating systems
- File systems
- Mobile phones (imaging, Operating Systems)
- Database systems, Data mining
- Malware Analysis
- Data concealing/disguising techniques
- Reverse engineering

F. Hacker Groups in Turkey

Ayyıldız Team (Ayyıldız Tim)

Ayyıldız Team founded in New Zealand in 2002 and operating in Turkey itself, patriotic, nationalistic, and is defined as the Kemalist Turkish hacker group. It contains many different groups and has a military rank system. The group announced its name by hacking the United States Department of Defense website. The team call themselves as soldiers of virtual world that they want to protect Turkey from future threats. By combining these statements with the idea of nationalism and using the anti-communist psychological warfare techniques of the Cold War, the group carries out hacking activities. They are especially known for their battle against RedHack and Anonymous. The motto of the group is a saying that Mustafa Kemal Atatürk also said, "He who loves his homeland the most is the one who does his job best." It is mentioned. Written about the group "Who is this Moon Star Tim?" There is one book named [69]

Redhack

“Redhack (Kızıl Hackerlar, Kızıl Hackerlar Birliği), is a Turkish Marxist-Leninist computer hacker group founded in 1997 the leader is K.M.Raif and the leader's the second pseudonym is MaNYaK. The group has assumed responsibility for hacking institutions including the Higher Education Council, the Turkish police, the Turkish Army, Türk Telekom, the National Intelligence Organization and many other blogs. The number of members of the group is said to be twelve. RedHack is the first band of hackers convicted of being a terrorist organisation and is presently one of the most sought-after communities of hackers in the world"[70].

B3yaz Hacker

"This hacker group uses a modification of the Turkish word for white, or beyaz, in its name in reference to white hackers (i.e. non-malicious hackers) who report vulnerabilities to manufacturers in order to make online systems more secure... On its website, the group announces that its staff is ready for Pentest87 requests. This is the only example in Turkey where a hacker group offers its hacking capabilities for a proper Pentest service. Since the penetration testing depends on trust, firms prefer to hire trustworthy private security companies, which can guarantee the protection of sensitive information regarding the firm. B3yaz Hacker's attacks can be divided into two groups. The first group of attacks is conducted to inform websites of their vulnerabilities. The second group of attacks are against websites that host content that are against the group's moral values. On Zone-H, there are several records under B3yaz.org, B3yaz, B3yazHacker, which contain 540 defacements in total on different websites with most of the attacks taking place in 2015. After inspecting the capabilities of B3yaz Hacker group, it is possible to say that it is not a treat to the nuclear power plants and critical infrastructure of Turkey" [54].

Turk Hack Team (Türk Hacker Team)

Türk Hack Team was founded in 2002 by Arsenik. The group is one of the oldest cyber team in Turkey. Its managers are said to be Bedros Sanches, OnLy, Arsenic, Se-Zer, Aksemsettin, ZoRoKiN, TheKar1zma, Corsair. The group did many offensive attacks in Turkey. They define themselves as a Turkish hacker group based on a Kemalist and nationalist basis. The group contains many hacking groups. Türk Hack Team announced its name by hacking MSN.COM, which was hacked and led by ZoRRoKiN as a first time [71].

Cyber Warrior (Akıncılar)

"Cyber Warrior, also known as Akıncılar93 (Turkish for "Raiders"), is a group that was established in 1999 with the name illegal-port. Later, they restructured this group under the name Cyber Warrior. The group's hierarchy mirrors that of the military. In one of the early recruitment calls of the group, Cyber Warrior's defined itself as a way of brotherhood" [54].

Turk Security (Türk Güvenliği)

Turkish Security is a hacking group established in 2009, focused on web and network systems. Its members are Turkish, and their total number is estimated to be around 5-10. Although it does not represent any segment in terms of political view, it is thought that it follows a statist and Islamic policy in terms of its actions [72].

PKK Hack Team

PKK Hack Team is a branch of the Kurdistan Workers' Party also known as Partiya Karkerên Kurdistanê (PKK). The PKK was founded as a Marxist-Leninist organization before turning into a primarily Kurdish nationalist movement over the course of the 1980s and 1990s.There is limited information on the PKK Hack Team regarding its online activities [54].

G. Cyber Crime Cases

Turkey Case 1 – Trial of Mahir Kanaat and Tunca Öğreten

Figure 4: On the left Mahir Kanaat and on the right Tunca Öğreten in the picture [76]

First Trial

Journalists Mahir Kanaat and Tunca Öğreten who have been detained for 323 days for publicizing the emails of the Minister of Energy and Natural Resources Berat Albayrak. Also, those journalists were charged with hacking e-mails of Albayrak in association with Redhack (hacker group) [22]. They committed the law of Art. 243 according to Turkish laws. Art. 243 (Accessing a data processing system), "Any person who unlawfully accesses, partially **or** fully, a data processing system, or remains within such system, shall be subject to a penalty of imprisonment for a term of up to one year or a judicial fine. [58]"

Second Trial

Figure 5: Picture from trial (Tunca Öğreten) [76]

All trials according to website of İstanbul Gerçeği [76]

Firstly, Mahir Kanaat was charged with Article 244 mainly (Preventing the functioning of a system), and Article

245(Misuse of bank or credit card). Secondly, Tunca Öğreten was charged with Article 244 mainly (Preventing the functioning of a system). The journalists who were in conviction without arrest could come to the hearing, but they were connected with Opinion and Teaching, Audio and Video Information System (SEGBİS). A statement was made in front of Çağlayan Courthouse for Kanaat and Öğreten, who had been deprived of their liberty for 347 days.

Trial starts

Mahir and Tunca will be connected to SEGBIS. That was the decision at the last hearing.
11.26 - The court came to the trial began.
Judge:

Public prosecutor; The nature of the offense, the existence of concrete evidence indicating the existence of strong suspicion that the offense was committed, the upper limit of the sentence imposed in the decision for the offense was considered, the judicial control provisions were insufficient, the defendants demanded the continuation of their detention.

Tunca Öğreten started his defense:
Right now, here is a journalist who communicates these emails with his professional constitutional rights without going beyond the basic principles and ethics of journalism. In other words, a journalist who has reached the data, made the necessary controls, shared with millions of people and gained publicity, and communicated the subject and the process. Moreover, a journalist who did not insult the minister and did not care about his private life ...
I have no close relationship with any hacker group. It has not been, nor is it possible. The fact that I have committed a crime on behalf of any organization is contrary to reason and logic. There is no evidence in the dossier that contradicts what I said. Another leak that has shaken the world has recently been reported. Paradise Papers in the name of the leak, the Canadian Prime Minister, Prime Minister Binali Yildirim, US President Trump, Queen of England directly or through the news was the subject. The information of their off-shore companies was shared with the world. The Queen's information was even communicated by the BBC, the state channel. A single journalist was neither detained nor arrested because of news that was similar to the news I made.
Mahir Kanaat started his defense:

I would like to start with the chat group that was originally created on Twitter but was actually created by the hacker group Redhack. My lawyers will present you with the sequel of the hacker group Redhack. As you can see in these twits, they write that they set up the chat group themselves. It is understood from the tweets that I did not set up the chat group and that the Redhack group did. Besides, why should I set up a chat group about e-mails that I don't even have? I will make a presentation on the downloading of the indictment of December 17-25. After this presentation, I'm sure there will be no doubt about it. This is not an issue that requires engineering knowledge.
Mahir Kanaat wanted to watch a video. The President of the court said, "Your lawyer will show up when he takes the floor."
The images were presented to the President of the Court.
We're entering the Google search engine. 17-25 December by writing the indictment 'enter' we press. As can be seen in 0.36 seconds 547 thousand results are seen. We are opening the http://www.adaletbiz.com/ page, which is frequently used by members of the judiciary. There are examples of the 17-25 December police enquiry reports mentioned in the indictment. (Meanwhile, Kanaat's lawyer shows the footage.)
Mr. President and members. I would like to talk about my attribute information. (Opinion proves that he did not upload images of the December 17-25 police enquiry reports to his computer before that date.) Downloaded from open sources. I have never had the slightest contact with any hacker organization. I'm not a Bylock user. I don't have a credit, credit card or bank account that I use in Bank Asya. How did I commit the crime of destroying evidence? I didn't include those emails. Therefore, I do not accept the crimes attributed to me as blocking the information system and destroying the data.
Let me give an example: There is a person who is arrested as a murderer and a trial is being made. But there's a problem here. There's no body and no killer. Can we be a murderer without murder? That's exactly my situation. There's no mail, but I'm accused of hacking the mail. I have been living in the same workplace for 14 years and in a fixed address for 8 years. There is no record in my record. I have two kids. I have a family to look after. For these reasons, I demand a free trial.
Mahir Kanaat's lawyer Tolgay Güvercin:
Mahir showed visuals. The CDs and flash disks we provide you with these images are in video format. The prosecutor did not mention the evidence. Because there's nothing to talk about. As a criterion of membership of the organization, the Court of Cassation deliberately and considers adopting the purpose of the organization. In this context, the Supreme Court of Appeals appears to make a material or moral contribution that is consistent.

Lawyer Güvercin presents examples of the decisions of the Supreme Court:
What evidence can you consider Mahir Kanaat as a member of the organization? The file is in front of you. Even if you download it today, the date will be the same as the police said. The date the police downloaded Mahir from his police enquiry reports after December 17-25. The police are actually denying themselves. Police, however, claim that Mahir downloaded the files before the investigations. The attribute information and the date the person downloaded the file are different. This is a very simple fact. If you download this information today, the attribute information seen on your computer will appear before the investigations. Our client clearly says. He says I'm a leftist. But he is accused of membership in a religious community. And there's no

evidence. Mahir can't be in this bag! Redhack clearly writes that they have seized these emails and formed a chat group. It's not RedHack himself. But journalists are still under arrest. Mr. Prosecutor must explain the evidence he claims to exist.

One of the lawyers of Kanaat, Lawyer Ali Deniz Ceylan began to speak:
We've been telling it since two sessions. There's only one evidence of crime. Keeping the files on December 17-25. These are not original documents. The prosecution says strong suspicion of crime continues. But we refute it every time. In other words, the probability of strong suspicion between the time we started trial and that time is unlikely to be the same. Doesn't the prosecutor have any doubts about it? If not, why do we have these conversations? Why are we discussing this evidence? The prosecutor should have a question against what we say. But not. According to the Constitution, the articles of the fundamental rights required by the international agreement, if the contracts contradict the law, the provisions of the contract are written. Turkey must implement the decisions of the Court.

Sevgi Kalan, Tunca Öğreten 's lawyer, started to speak:
We objected to the defense with SEGBIS. He was supposed to be present. You had to have a serious reason for your decision. As a matter of principle, he was supposed to be here. You're violating your right to a fair trial. The prosecutor decided in a puzzled way, we are concerned. The prosecution asked to continue detention on standard grounds. He's been in prison for a year, but there's no evidence. The client did not capture the emails. Redhack has released. There are explanations about this. And there are thousands of stories about it. The client follows an agenda on the subject and has correspondence with journalists nearby. Now here the client under the file is an organization link, liaison has nothing.
One of the lawyers of Kanaat, Tolgay Güvercin took the floor:
You decided about the expert. Exactly a month passed, the expert did something. We stopped by your pen every day in a month. Two days before the hearing, the expert wrote. You wrote the answer yesterday. Despite the period of one-month special pen and you did not ask. Mr. President, this research hasn't been done in a year. You decided a month ago. We showed you visuals. Flash has video. You don't need an expert if you watch a video. You will still want an expert, make a criminal complaint against the expert who is not doing his duty.

The court interrupted the hearing for an interim decision.
The court`s decision is to release for Tunca Öğreten and Mahir Kanaat!

Figure 6: People protesting in front of the court building [76]

Turkey Case 1 – Trial of Mahir Kanaat and Tunca Öğreten (Indictment)
All indictment according to [87]

Title: Emails of The Minister of Energy and National Resources were hacked by Redhack group. Journalists Mahir Kanaat and Tunca İlker Öğreten were charged with being part of the group and publicizing the emails.
Related Law
Art. 244.- Preventing the functioning of a system (Main focus of crime)
Art. 240.- Avoiding the sale of goods or services
Art. 243.- Accessing a data processing system
Art. 314.- Armed Terrorist Organization
Art. 58.- Repetition in crime and special dangerous offenders
Art. 53.- Deprivation of certain rights
Art. 63.- Deduction

Relevant information

When evaluating the case, in the light of this information and evidence which are subject to investigation the Republic of Turkey of Energy and Natural Resources Minister (Berat Albayrak) `s passwords of email addresses were hacked in September of 2016, in particular the DHKP-C terrorist who themselves Redhack name is connected with it. The organization dealt with by hackers group obtained the data and information and manipulated them to impact on Republic of Turkey Energy and Natural Resources Minister. Energy and Natural Resources Ministry`s information related to its strategic activities and operations that are manipulated and thereby the energy policy and the creation of Ministry were shown as failure and as corrupted in government of the Republic of Turkey. It was understood that the aim and the act could not be realized by a single suspect in the case where the Minister tried to establish the perception that the Minister of Affairs was associated with the ISIS terrorist organization. In this case, the subject of the investigation is a very perpetrator of the crime, information and technical competence is available and the decision about the suspects of unknown perpetrators mentioned in the previous parts of the indictment as described in the hacked email. Then, created a piece of digital data via a social network called twitter where all the suspects whose indictments were issued

at this stage were unlawfully seized. These aims of suspect are clarifying evidence that these characteristics of the data obtained by the illegal methods. Also, the social and educational status of the suspects validates that they can have knowledge to access data illegally. Therefore, as mentioned in their defense, these activities cannot be considered as journalistic activities. It is considered that they have committed the crimes stated in Article 244.

Case details of Mahir Kanaat

It was found that the account named @mkanaat mentioned in the notice text appeared on the Twitter account named Mahir Kanaat with ID number 459071271, and in the research, it was found that the person using the said profile was Mahir KANAAT. SAMSUNG brand mobile phone image captured from the search results of the suspect. In the instant messages and e-mails section, it is determined that there are records of direct communication with two different persons mentioned in the above-mentioned notice. Again, in the examination of the image of the mobile phone seized from the suspect named Mahir KANAAT related to @Mkanaat Twitter account of Mahir KANAAT on the "Followed" and "Followers" tables. It was found that the various profile pages of the hacker group called RedHack, which are the subject of the notification, are mutually followed and thus the suspects are in direct communication with the hacker group that performs the hacking of the mails subject to the notification. In the examination of the suspect's contact list, it was found that the other persons who were notified were registered in the contact list.

In the examination of the image of the mobile phone seized from the suspect named Mahir KANAAT, while the FETÖ / PDY was serving in the cadres of the armed terrorist organization Istanbul Security Directorate, the law enforcement officers police enquiry report on the operations of 17/25 December 2013 for the purpose of overthrowing the selected legitimate government under the legal investigation view. In this context, the report on December 17 operation was created during the 80-hour working period from 09/09/2013 to 22/09/2013, the original report is not possible to be found on the internet and only if FETÖ / PDY It is possible to seize the members of the units, as well as the FETÖ/ PDY structuring of the operation on December 25, 2013, the report example of the operation was seized on the suspect's computer, the nature of the file. When the operation report which was planned to be made on December 25, 2013 was created on 17/12/2013, as mentioned in the previous paragraph. This file, which is an example of this original report, can only be obtained from the FETÖ/PDY members, so that the suspect can. It was considered that the seizure of the report of some of the law enforcement documents which had not been made even before the operation date. The documents were evidence that the suspect was a member of the said FETÖ/PDY armed terrorist organization and carried out some duties on behalf of this organization.

In the investigation on the mobile phones that the suspect used. It was determined that there were telephone communications with the suspect named İlker Deniz YÜCEL, who was being investigated for the same incident, which was given a decree regarding the investigation documents. The documents are referred to above are subject to notification of the defense received the suspect is using itself the last twitter account. The consent of that outside of twitter is added to a group through the portal, this group in the Republic of Turkey The Minister of Energy and National Resources Minister Berat Albayrak's account to a different e-mail on which the migrated mail was addressed on user name and It was determined that the password was distributed, again in this group of correspondence in which these mails will be distributed or speculated to be given some instructions. Then, he left the group stated that he did not accept the allegations mentioned in the notice.

Case details of Tunca İlker Öğreten

It was found out that the account @tuncaogreten mentioned in the notice text appeared on the Twitter account named Tunca ÖĞRETEN, ID 69797292, and that the suspect used this account was determined as a result of the research. In the examination of the APPLE Brand Laptop image, replacement of mails in the zip file were seized from The Minister of Energy and National Resources Minister by the suspect. However, the investigations carried out on digital materials that seized from the suspects. According to his fiancé and a friend of his, these interviews with the suspects in dialogue with the parties addressed to those hackers named RedHack proclaimed that the investigation on the materials obtained from the suspect. It is determined that some of the other persons subject to the notification in the list of persons are attached. In defense received the suspect, of the above are subject to notice the twitter account that he used the consent of that outside of twitter is added to a group through the portal, The Minister of Energy and National Resources Minister (Berat Albayrak) `s mails were downloaded by following the link on which the migrated mail was addressed. Then, the suspect did not accept the allegations mentioned in the notice. In the HTS examination of the suspect, it was found that the suspect had contact and communication with İlker Deniz YÜCEL, whose investigation documents were classified, and the suspect was in contact with the other suspects were subject to the investigation.

The DHKP-C armed terrorist organization has illegally obtained information which may also be in the form of personal data and, if necessary, state secrets, by communicating the data obtained by the suspect in the manner described above. The suspect got help by the hacker group. Then, the suspect Tunca İlker Öğreten was in contact with the hacker group REDHACK that investigation of the computer proves. Also, he has already worked in the news site Diken.com.tradlı, previously FETÖ/PDY armed terrorist organization, who is determined to work in the newspaper TARAF newspaper as well. The suspect was a member of

both organizations with the acts committed organizations in line with the purpose and ideology of the crime committed. It was evaluated that he had committed a crime on behalf of the organization.

Sentences

First Trial
Journalists Mahir Kanaat and Tunca İlker Öğreten have been detained for 323 days.

Second Trial
The court`s decision was to release for Tunca İlker Öğreten and Mahir Kanaat

Turkey Case 2 – Trial of Duygu Kerimoğlu, Alaaddin Karagenç, and Uğur Cihan Okutulmuş

Figure 7: RedHack Organization [20]

At the trial's first session yesterday, three pupils who had been held behind bars for nine months on allegations of being employees of the leftist hacker group RedHack were released. With fresh launches, all 10 offenders are now safe to proceed while the request of the Interior Ministry to be approved as an interfering group has also been approved.

The RedHack investigation was initiated after a cyber-attack was carried out by the group on the website of the Ankara Police Department in February ; attorneys demand up to 24 years in prison for suspected offences of the accused. Suspects were initially detained in March on charges of "committing a crime in the name of an armed terror organization despite not being a member of a terror group." RedHack has consistently said those on trial have nothing to do with the organization. [73]

All trial according to the websites of Hürriyet [77] and Başka [78]

Notes from Trial
Duygu Kerimoğlu, Alaaddin Karagenç, and Uğur Cihan Okutulmuş were charged with Article 244 mainly (Preventing the functioning of a system). Prosecutors are demanding up to 24 years in prison for the suspects. Ankara 13 High Criminal Court 8 defendants and lawyers participated in the hearing, 3 of the detained. The President of the Court summed up the indictment at the beginning of the hearing, saying that the accused were charged with membership of an armed terrorist organization, committing crimes on behalf of the organization and committing various IT crimes.

Figure 8: Alaaddin Karagenç in the picture [80]

Alaaddin Karagenç started his defense:
I am not a member of any illegal terrorist organization and organization. I did not help such organizations. I did not enter the Ankara Police Department illegally. I have no such action. There is no evidence that I have entered the Ankara security site or that I have stolen documents. Curiosity is the most basic human characteristic. Little children put their hands-on fire out of curiosity. We live in the age of informatics today. We can access all kinds of information on the Internet. I go to hundreds of sites a day. That's how I met Redhack. That's how I met Maniac. From time to time I was in the chat rooms. But I have not received any instructions and orders about them. My main goal in these chat rooms was to get knowledge of technological issues. I didn't even know that the man with the nickname was guilty. I entered this site to enter technological issues. This investigation begins on notice. What is the credibility of the whistleblower? He calls me Alaaddin from Marash(City of Turkey). Very unfounded notice was made. We were arrested for not informing evidence. We have collected information on notices. I knew Redhack from the Internet, out of curiosity. I did not enter Ankara Police Department and did not steal the information illegally. There's no evidence in the file. I've been under arrest for nine months. I'm the victim. If he called safety, I'd give him information. I was wrongfully arrested. I want my release.

Figure 9: Uğur Cihan Okutulmuş in the picture [80]

Uğur Cihan Okutulmuş started his defense:

I did not break into the Ankara Police Department's site without permission. My ability to use computers is not enough to bring down the site. There are not programs on my computer that will crash the site. There is no evidence that I entered the website of the Ankara Police Department from my computer. I do not use the nickname Kızılcan Yıldız (Crimson Star). The person who uses this name is also the person who uses the name Maniac. I learned from Facebook that the Ankara Police Department entered the site. There is no accusation that I entered the site in the expert report about me.
After entering the site of the Ankara Police Department, I talked with a person called Manyak(Maniac) on an online chat site. This conversation happened after the safety site collapsed. The conversation between us is about uploading a news video made by NTV to You Tube. I also found out that Redhack had a charter. I don't know any of the defendants. I'm a senior in high school. I've been under arrest for nine months. I've suffered enough. I want my release to avoid any further victims.

Figure 10: Duygu Kerimoğlu in the picture [79]

Duygu Kerimoğlu started his defense:
I have two computers to follow my classes. In my investigation, two laptops and desktops were confiscated. The accusations against me are some articles, some news I read. The charges against me are unfounded. I don't even know Redhack members online. I did not hack the site of the Ankara Police Department. You need to have high level computer knowledge to do hacking. I don't know how to hack. I don't even have computer programs to hack. If I had this level of computer knowledge, I wouldn't be in the fifth year of a two-year school. All I did was read the news about Hack. I did this to get information. Evidence has been made by distorting a comment on Facebook. From this comment, it is claimed that I know Redhack. However, this claim is not true. I don't know Redhack's charter. I did it on February 20th. At that time, there was no event of entering the security site.
The court decided to release the defendants Duygu Kerimoğlu, Alaaddin Karagenç and Uğur Cihan Okutulmuş.

Turkey Case 3 – Turkish High School Student committed law (Mischief to Data and Illegal Access)

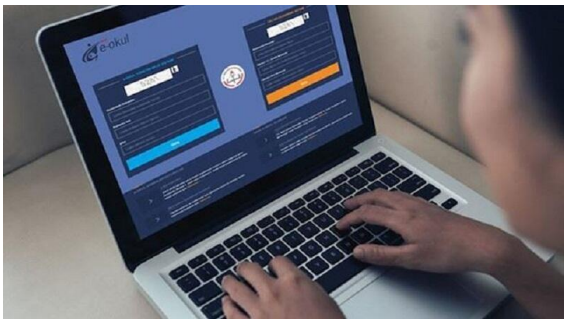


Figure 11: Picture of e-okul application [74]

10th grade student, hacked the Ministry of Education's grading system a week ago in Diyarbakır which is city of Turkey. Grading and absenteeism changed the student's hacking process by the school administration. Kayapınar district of Diyarbakır of absenteeism for about 2 months 10th grade student Sultan Şeymus M. She allegedly hacked the system of the Ministry of National Education. Here, the student's grades increased by per 20, then the absence of 59 days to 9 days reduced. Teachers who graded the student, corrected the system, thinking that the problem was school system and made to restore the system. Sultan Şeymus M. re-entered the system the next day, notes and absenteeism again attracted the attention of the school administration when updated by itself. After the notice to the police Directorate of Cyber Crimes teams took note of the system. She is detained After the work of Sultan Şeymus M. 's home, the security forces who detected that the system entered the IP address, detained the student. 10th grade student Sultan Şeymus M. was released after the police statement [74].

Turkey Case 4 – Armenian exchange student arrested in Istanbul on child pornography charges
An Armenian medical pupil who was part of an internship program at the Cerrahpaşa Faculty of Medicine at the University of Istanbul was detained for supposedly downloading and exchanging child pornography, reported daily Habertürk on Jan. 15. The 24-year-old suspect was detained by police in an operation after intelligence shared by the U.S.-based National Center for Missing and Exploited Children (NCMEC), a non-profit organization that deals with missing and sexually exploited children. Having recognized the suspect's IP address, the NCMEC informed the Turkish officials of information on how to locate the applicant, after which he was discovered and arrested by police officials. The accused rejected the accusations and was discharged as his laptop and hard drives were encrypted due to encryption. Following a lengthy investigation undertaken by cybercrime police units, the codes on his computer were cracked and thousands of child pornography images were found. The Istanbul Prosecutor's Office granted a second arrest warrant and the accused was detained on allegations of "downloading, storing, and exchanging pictures of child abuse through access to prohibited websites [86].

Turkey Case 5 – 334 years in prison for identity theft and banking fraud, in turkey a man received the most severe sentence for committing a cyber crime

Figure 12: The picture of Onur Kopçak [89]

Named Onur Kopçak, the hacker was detained in 2013 for running a phishing blog that impersonated a bank account, tricking people into offering their bank details including data on credit cards. A latest situation in Turkey shows that logging can be a hazardous operation. A 26-year-old Turkish carder has been convicted to a consecutive imprisonment for 334 years in total, he has been convicted to defraud 54 clients through identification robbery and loan scam. Onur Kopçak, this is the man's title, will be in prison in Turkey for the remainder of his life. The Turkish press report Onur Kopçak got 199 years and seven months in 2013 from the Criminal Court of Appeals for stealing 43 credit cards through a phishing scheme abolished by the Criminal Court of Appeals. Obviously, the person professes his guilt, this is the harshest sentence for committing a cybercrime. Albert Gonzalez was convicted to 20 years in prison in 2010 for orchestrating a huge U.S. bank robbery, while Silk Road mastermind Ross Ulbricht was convicted to life imprisonment [89].

Turkey Case 6 – The website employee was sentenced to 18 years in prison for voyeurism.

News and e-mail service in a widespread Internet site in Sariyer office 'voyeurism' shock was experienced. Allegedly, employee Özgür Ç., placed hidden cameras in the toilet that shared men and women and blackmailed employees with images obtained. Company lawyers brought the case to court. The Istanbul Public Prosecutor's Office's investigation lasted for 5 months and evidence was collected and the defendant Özgür Ç. His statement was taken from April 2017 to December, said that he worked in the company. Then, Özgür Ç. mentioned, "My colleagues working in the company was constantly complaining to my superiors. I thought that the complaint was made by phone. The only indoor area can be talked by phone. Therefore, I placed a camera in the toilet. I did not send images to any site, did not blackmail anyone," he said. in the search of residence of Özgür Ç, a large number of flash memory, hard disk, laptop, desktop computer, mobile phone, lines, hidden camera features, CD cards, CDs and DVDs were seized. The material was also found in the investigation of a large number of violations of private privacy and obscenity found inappropriate images of women and children. At the end of the investigation carried out by the prosecution Özgür Ç. about, "Sexual Harassment, Violation of the Privacy of Private Life and Disclosure, Violation of Freedom in Work, Blackmail, Mediation for the publication of obscene publications, Obscenity through Child Pornography" indictment was held. In the case, 20 people involved in the site took part as victims. The trial in Istanbul Criminal Court of First Instance has been completed recently. The court, 7 months 10 days detained Özgür Ç. 7 years 6 months on the charge of violating the privacy of private life, 10 years 6 months and 4 thousand 500 days on the crime of obscenity hit a judicial fine. The court did not postpone the sentence, considering the severity of the offense of Özgür Ç. (above the legal limit of the sentence imposed) [90].

SWEDEN

A. Legal and Judicial System in Sweden

Swedish Judicial System

The legal framework is ordinarily taken to comprise the organizations in charge of guaranteeing the standard of law and lawful security. The courts structure the foundation of this framework. Organizations for crime investigation and prevention., the Swedish Police Authority, the Swedish Crime Victim Compensation and Support Authority, the Swedish Security Service, the Swedish Prosecution Authority, the Swedish Prison and Probation Service and the Swedish Economic Crime Authority are likewise viewed as a major aspect of the legal framework. Different offices, for example, the National Board of Forensic Medicine and the Swedish Enforcement Authority, may as well have duties inside or connected to the legal framework [91].

Court System

The Swedish judiciary has approximately 6,400 staff dispersed among approximately 80 separate judiciary, officials and commissions.

There are three types of courts in the Swedish Judicial System:

The general courts (the Supreme Court, District Courts, Courts of Appeal).

District courts are the basis among the public judiciary, dealing with criminal, civil cases and other issues of multiple types. Sweden has about 46 district courts, they differ in volume, ranging from about tens to hundreds of staff members. Five district courts have land and environment courts, hearing instances and problems dealing with e.g.

environmental and water problems, property registration, scheduling and construction problems. Regarding their court of appeal, there are six of them [91].

The administrative courts (the Supreme Court, the Administrative Courts and the Administrative Courts of appeal and)

General administrative courts cope with instances concerning society and individual conflicts. There are twelve of these administrative courts in which four of them house migration courts as well.
The last resort tribunal is the Supreme Administrative Court. It comprises of at least 14 judges. The main job of the Supreme Administrative Court, like the Supreme Court, is to generate precedents. For most types of cases, leave to appeal is necessary [91].

The special courts (e.g. Foreign Intelligence Court, Labor Court).

Tenancy Tribunals and Regional rent are administrative officials with duties of a court-like nature. In such conflicts, a regional rent tribunal examines certain tenancy conflicts and conflicts over tenant ownership and mediates or acts as the arbitral court [91].

B**. International Affairs**

Security Divisions

CERT-SE is the Computer Emergency Response Team handling the computer security incidents in Sweden. Their tasks are to support the community on preventing IT incidents by handling urgent IT incidents, interacting with authorities regarding information security and cooperating internationally with other Computer Security Incidents Response Teams (CSIRT). Usually, the Swedish Agency for Social Protection and Preparedness (MSB) is where IT operations are conducted [92].

International Cooperation

In Swedish police operations, international police collaboration is playing an increasingly significant role. In the following four fields, the Swedish police are mainly involved.

Cooperation with foreign police organizations

International operational police collaboration implies that the Swedish police collaborate with international police organizations, e.g., directly or through Europol, Schengen cooperation, Interpol or Nordic police collaboration [91].

International strategic police cooperation

In this field, Swedish Police cooperate and coordinate the work of institutions, primarily within the EU, who have a role in police activities. This job generates stronger circumstances for Member States ' security organizations to fight increasingly varied and organized cross-border crime together [91].

International development cooperation

International development cooperation implies that the Swedish police are supporting overseas police organizations in their attempts to become more democratic and efficient. The Swedish police are helping to build a police organization in a foreign country that supports and preserves human rights, maintains the rule of law, can be kept responsible and provides the greatest consideration to the requirements of people. This practice also contributes to the development of the Swedish police [91].

Peace support and conflict prevention

Peace support and conflict prevention means that Swedish police officers are serving in peace and conflict prevention activities throughout the UN, the EU and the OSCE [91].

Europe Courts

The European Union's Court of Justice is situated in Luxembourg. The Court has two primary duties: to resolve conflicts between EU institutions and Member States and to apply EU law.

It is made up of three judicial institutions:

- Court of Justice
- General Court
- Civil Service Tribunal

The European Court of Human Rights (ECHR) is situated in Strasbourg, it has 47 Member States. The ECHR can examine States ' responsibilities under the European Convention on Human Rights to fulfill their commitments. The European Court of Human Rights ' rulings are legally binding on the State in question. The European Court of Human Rights may obtain claims from people, NGOs or organizations who think their rights have been breached. Neither the European Union Court of Justice nor the European Court of Human Rights is higher to the Swedish court and authorities in Sweden. Therefore, a Swedish court's judgment cannot be appealed to them. Nor can they undo judicial judgments or decisions taken by national authorities [91].

C. **Swedish Law Related to Cybercrime**

Penal Code [93]

Chapter 4 – On Crimes against Liberty and Peace

Section 7 - Anyone who physically harms someone else or exposes someone else to disturbing contacts or other reckless conduct is convicted, if the act is apt to violate the victim's peace in a tangible way, for non-payment of a fine or imprisonment for a maximum of one year. Law (2017: 1136).

Section 8 - A person who unlawfully obtains access to a communication which a postal or telecommunications firm delivers or transmits in the form of mail or as a telecommunication, shall be sentenced for breach of postal or telecommunication secrecy to a fine or imprisonment for at most two years. (Law 1993:601)

Section 9a - A person who, in a case other than as stated in Section 8,unlawfully and secretly listens to or records by technical means for sound reproduction, speech in a room, a conversation between others or discussions at a conference or other meeting to which the public is not admitted and in which he himself does not participate, or to which he has improperly obtained access, shall be sentenced for eavesdropping to a fine or imprisonment for at most two years.(Law 1975:239)

Section 9b - A person who employs technical means with the intention of committing a breach of telecommunication secrecy in the manner stated in Section 8 or to commit a crime as defined in Section 9a, shall be sentenced for preparation of such a crime to a fine or imprisonment for at most two years if he is not responsible for a completed crime. (Law 1975:239)

Section 9c - A person who, in cases other than those defined in Sections 8 and 9, unlawfully obtains access to a recording for automatic data processing or unlawfully alters or erases or inserts such a recording in a register, shall be sentenced for *breach of data secrecy* to a fine or imprisonment for at most two years. A recording in this context includes even information that is being processed by electronic or similar means for use with automatic data processing. (Law1998:206)

Section 10 - Attempt, preparation or conspiracy to commit kidnapping, unlawful deprivation of liberty or placing a person in a distressful situation, and any failure to reveal such crimes, shall be adjudged in accordance with the provisions of Chapter 23. The same shall apply to an attempt or preparation to commit unlawful coercion of a serious nature or breach of data secrecy, which if it had been completed, could not be considered petty. (Law 1998:206)

Chapter 8 – On Theft, Robbery and Other Crimes of Stealing

Section 1 - A person who unlawfully takes what belongs to another with intent to acquire it, shall, if the appropriation involves loss, be sentenced for theft to imprisonment for at most two years.

Section 12 - An attempt or preparation to commit theft, gross theft, robbery, gross robbery, vehicle theft or unlawful diversion of energy, and also conspiracy to commit or failure to reveal robbery or gross robbery shall be punished in accordance with the provisions of Chapter 23. If, however, a completed vehicle theft would have been regarded as petty such punishment shall not be imposed.

Chapter 9 – On Fraud and Other Dishonesty

Section 1 - If a person by deception induces someone to commit or omit to commit some act which involves gain for the accused and loss for the deceived or someone represented by the latter imprisonment for at most two years shall be imposed for *fraud.* A sentenced for fraud shall also be imposed on a person who, by delivering incorrect or incomplete information, or by making alterations to a program or recording or by other means, unlawfully affects the result of automatic data processing or any other similar automatic process so that gain accrues to the offender and loss is entailed by any other person. (Law 1986:123)

Section 6 - A person who, takes possession of something of which another has been dispossessed by a crime, and does so in such a manner that the nature thereof renders its restitution difficult,2. procures an improper gain from another's proceeds of crime,3. improperly promotes the opportunity for another to take advantage of property emanating from the proceeds of crime, or the value of such property,4. assists in the removal, transfer, or sale of property which is derived from the proceeds of crime, or takes some similar measure, with the intent of concealing the origin of property, or5. by a demand, transfer or other similar means asserts a claim arising from a crime, shall be sentenced for receiving to imprisonment for at most two years. A person who, in business activities or as a part of business activities which are conducted habitually or otherwise on a largescale, acquires or receives something which may reasonably be assumed to have been misappropriated from another person by a crime, and does so in such a manner that the nature thereof renders its restitution difficult, shall be similarly sentenced for receiving. If the crime referred to in the first or second, paragraph is gross, imprisonment for at least six months and at most six years shall be imposed. (Law 1993:207)

Chapter 13 – On Crime Involving Public Danger

Section 4 - A person who destroys or damages property of considerable importance for the defense of the Realm, public subsistence, the administration of justice or public administration, or the maintenance of public order and security in the Realm, or by some other action, not limited to the withholding of labor or encouraging such action, seriously disturbs or obstructs the use of such property, shall be sentenced for sabotage to imprisonment for at most four years. This shall also apply if a person otherwise, by inflicting damage or by other action of the kind just described, seriously disturbs or obstructs public traffic or the use of telegraph, telephone, radio or other similar public service or use of an installation for the supply of water, light, heat or power to the public.

Chapter 16 – On Crimes against Public Order

Section 10a - A person who

1- portrays a child in a pornographic picture;
2- disseminates, transfers, grants use, exhibits or in any other way makes such a picture of a child available to some other person;
3- acquires or offers such a picture of a child;
4- brings about contact between a buyer and a seller of such pictures of children or takes any other similar step to facilitate dealing in such pictures; or
5- possess such a picture of a child

shall be sentenced for child pornography crime to imprisonment for at most two years, or, if the crime is petty, to a fine or imprisonment for at most six months. By child is meant a person whose pubertal development is not complete or, if it is apparent from the picture and its attendant circumstances, who is less than 18 years of age. person who in the course of business or otherwise for the purpose of making money disseminates a picture of the kind described in the first paragraph through negligence shall be sentenced as there stated. If the crime described in the first paragraph is considered to be gross a sentence of at least six months and at most four years shall be imposed for gross child pornography crime. In assessing whether the crime is gross special consideration shall be given to whether it was committed in the course of business or otherwise for profit, was a part of criminal activity that was systematically practiced or practiced on a larger scale, or concerned a particularly large number of pictures or pictures in which children are exposed to especially ruthless treatment. The prohibitions against depiction and possession do not apply to a person who draws, paints or in some other similar hand-crafted fashion produces a picture of the kind described in the first paragraph as long as it is not intended for dissemination, transfer, granted use, exhibition or in any other way be made available to others. Even in other cases the act shall not constitute a crime if, having regard to the circumstances, it is justifiable. (Law 1998:1444)

Section 10c - Any person who, intentionally or through gross negligence in the course of business or otherwise for the purpose of making money purveys to a person under the age of fifteen a film, video recording or other technical recording with moving pictures explicitly and realistically depicting violence or the threat of violence towards humans or animals shall be convicted of illicit purveyance of a technical recording and sentenced to a fine or imprisonment for at most six months. The provisions of the first paragraph do not apply to films or video recordings approved by the National Board of Film Censors for showing to children under the age of fifteen. Nor shall they apply to a technical recording of moving pictures with an identical content to a film or video recording approved by the Board of Film Censors. In addition, the first paragraph does not apply to public showings of films or video recordings. If a technical recording of moving pictures is furnished with a certificate confirming that a film or video recording with an identical content has been approved by the National Board of Film Censors for showing to children under the age of fifteen, no criminal responsibility exists under the provisions of the first paragraph. This shall not, however, apply if the certificate was false and the person who purveyed the recording realized or should have realized that this was so. (Law 1998:1444)

Section 12 – A person who distributes among children or young persons a writing, picture or technical recording which owing to its content may brutalize or otherwise involve serious danger to the moral nurture of the young, shall be sentenced for leading youth astray to a fine or imprisonment for at most six months. (Law 1998:1444)

D. Cybercrime Court Cases

1) The Pirate Bay Trial

The Pirate Bay (TPB) is a website containing an online index of various types of content such as entertainment media, games, software and books. It was founded in 2003 by the Swedish think tank Piratbyrån, to support free sharing of information. Users in this website can search and download torrent files, as well as contribute files, facilitating peer-to-peer (P2P) file sharing amongst users using the BitTorrent protocol, a communication protocol for P2P sharing [94].

Summary

On the 31st of January 2008, Swedish prosecutors file charges against Gottfrid Svartholm, Fredrik Neij, Peter Sunde and Cart Lundstrom, a Swedish businessman who used to sell his services to TPB [95]. The reason for the charges is that the prosecutors believed the members of TPB were facilitating breach of copyright, whether it be for themselves or other people's breach of copyright. Many cases of copyright infringements were listed during the trial, the majority were linked to music, and the rest were related to games movies

and games [96]. The trial debuted on the 16th of February 2009, the case was trialed in the Stockholm District Court in Sweden, it was decided by a judge and three lay judges. Hearings were finished on the 3rd of March 2009, and the verdict, announced on the 17th of April 2009. All four accused were found guilty and sentenced to one year in prison, as well as a fine of 30 million SEK [97]. The verdict was appealed and in November 2009, the appeal went through, and prison sentences were shortened, but damages were increased.

Trial

More detail on the case, on the 31st of May 2006, Swedish police raided TPB in twelve different premises. 186 servers were confiscated, this caused TPB to go down for three days. In 2007, a report was produced in preparation for the trial, containing 4000 pages of information relating to payments, emails, SMS messages, documents, screenshots of TPB and police interrogation records [98]. During the trial, half of the charges were dropped by the 2nd day due to lack of evidence, dropping charges relating to assistance of copyright infringements, leaving only the assistance of making copyrighted work available. On the 3rd day of the trial, Per Samuelson, who was the defense attorney, gave an argument that was later dubbed the "King Kong" defense [99]. The defense attorney stated from EU directive 2000/31/EC [100], a person who provides information services will not be responsible for transferred information unless that person initiates the transfer himself. This argument was dubbed as the King Kong defense because Samuelson gave a scenario example of a real user from TPB whose username was "King Kong" and could have been living in Cambodia. But in its April verdict, the court decided not to apply the EU directive since the defendants had collective responsibilities for TPB and were aware some torrent files were subject to copyrighted material [96]. The Prosecutor team attempted multiple times to bring a new witness to the case as well as new evidence, the judge decided that the prosecution had to hand over the new material since it has not been shared with the defense and the court before the trial started [101]. For the remaining days of the trial, the prosecution tried to present TPB as a huge profitable business that made money from assisting people who violate the copyright law. As for the defense, they attempted to show TPB simply as a search engine like google, therefore subject to the same protections.

Verdict and Appeal

The accused were all guilty of "accessory to crime against copyright law". However, the prosecutor never tried to prove a crime was committed, but rather a person was an accessory to the crime. The court stated, "responsibility for assistance can strike someone who has only insignificantly assisted in the principal crime". The entertainment industry lawyers and the defense lawyers appealed the verdict. The first appeal was on the 28th of September 2010, and verdict announced on the 26th of November 2010, the defense succeeded in trading some of the jail time to increased fines [96]. The accused were all judged individually due to individual contribution of the facilitation of illegal file sharing; 10 months of jail time for Fredrik Neij, 8 months for Peter Sunde, 12 months for Gottfrid Svartholm and 4 months for Carl Lundstrom, as well as under one million dollars each [96]. The appeal from the prosecutor also succeeded in increasing the fines to about 46 million Kronor. Another appeal from the defense was set for Sweden's Supreme Court but was not successful, and that any further appeals would be rejected by the court.

2) Recording of Intimate Interaction

Summary

For the purpose of maintaining identity privacy, the full names of the people involved in this case were not shown, the names have been replaced with initials instead. The accused (AB) is a Mexican citizen born in 1967, he was summoned to trial at Solna District Court, for defamation, fraud and unlawful interception. The two victims in this case are MM, who was previously in a relationship with AB (AB did not realize the relationship was over), and JC who also had relations with MM. The Supreme Court gave the final verdict, AB was given a penalty fine of 385 SEK [102].

Trial

In May 2003, AB installed a hidden camera and microphones at MM's residence in Ballonggatan, Solna. From May 9 to 28, AB has been illegally recording conversations and meetups between MM and JC at the residence. Various sessions were recorded, such as private discussions between the two victims, as well as sexual intercourse. AB has set up the recording equipment in a way MM or JC would eventually realize. After these events, AB retrieved the recorded material and proceeded to sharing them via e-mail to several friends and family members of MM, along with a letter stating how MM was unfaithful to him. More emails were sent during May, to six colleagues of AB, containing images of MM with JC at the residence [102].

During trial, AB admitted on installing the equipment, however denied any responsibility for the crime on the grounds that the interception took place in a joint residence between him and MM, and therefore, was not unlawful. Regarding the prosecution for slander, AB disputed responsibility for the crime since the crime itself was committed in Mexico, from which the emails were sent and therefore not punishable in Sweden. AB also mentioned JC was neither named nor identified in the recordings he sent via email [102].

Following the court's assessment, AB was convicted of unlawfully intercepting or recording speeches in a room, of installing recording equipment without MM's knowledge nor

consent. Regarding the captured images, there is no prohibition in Swedish law for photographing individuals without consent, thus the dismissal of this charge. Even though AB sent the emails from Mexico, the prosecutor indicates the emails were still received in Sweden. AB was also guilty of slander by sending offensive emails regarding MM to her family members, however JC was not subject to slander since he was not included in the emails. Regarding the emails sent to the six colleagues, there is no proof but the denial from AB of sending any form of sexual content, and therefore the prosecution for defamation was rejected [102].

Verdict and Appeal

AB was sentenced for unlawful eavesdropping and slander, as well as a fine of 385 SEK and other undefined fines to both MM and JC. Both the prosecutor and defense filed for appeal to the Svea court. The prosecutor requested AB to be convicted for misconduct of MM and JC, in order to increase the severeness of the sentence. AB appealed for the dismissal of both sentences, unlawful interception and slander. The appeals were held at the High Court, with Court Judge Assessor Anders Hübinette. AB proceeded with similar reasons than during the trial in District Court, saying the residence was joint between him and MM, and that the letter addressed to MM's family were not intended to disrespect MM in any way. The High Court agreed with both of the sentences given by the District Court and decided the ruling regarding these charges shall remain firm. The outcome of this case resulted in an additional punishment, AB was condemned for fraud. The damages were also determined, AB had to pay 41,000 SEK to MM and 26,000 SEK to JC, plus interested in accordance to the Interest Act, from 31st of May 2003 [102].

AB appealed the previous sentence to the Supreme Court, asking for the dismissal of the indictment and the fines he had to pay to the victims. Regarding unlawful interception, MM and JC's personal integrity could not clearly be defined and was too vague for the charge to be applied since this case was unique and the applicable laws were not fitting the scenario. For the distribution of images, it was noted that the ruling from the District Court lacked evidence, there was not enough proof that the emails sent to friends and family members contained the alleged images and the prosecution was therefore rejected. Concerning the charge of fraud, it was debated whether fraud by reckless conduct could be considered criminal, and since the confusion lead to multiple interpretations of the act, for the sake of legality, the court decided to dismiss the sanctions regarding fraud. The final verdict concluded on the 23rd of October 2008, and AB was left with a penalty of 385 SEK [102].

3) Possession of Child Porn

Summary

For the purpose of maintaining identity privacy, the full names of the people involved in this case were not shown, the names have been replaced with initials instead A patient from the Regional Psychiatric Clinic in Växjö was convicted with possession of child pornography. Suspicion arose while NN (the accused) was a patient at their clinic. The clinic visited the patient's room and found USB flash drives containing child pornographic images and were given to the Prosecutor's Office [103].

Case

After the clinic handed over the evidence, NN filed a complaint against them for taking and disposing his USB flash drives during his stay on the 17th of August 2011. More information about NN was given by the clinic to Chamber Prosecutor Johnny Philipsson. A house search was also carried out at the clinic, where materials were confiscated. From what other patients reported, NN was still withholding child porn in his room and thus more searches were conducted, gradually disposing of the pornographic materials and handing it over to the judiciary. Following the complaint from NN, the County Council gave their reasons; NN was previously sentenced to psychiatric care for rape, child pornography and gross sexual exploitation of underage. The forensic psychiatric investigation describes NN as being a pedophile, suffers from personality disorder, as well having autistic, narcissistic and paranoid traits [103].

This was not the first time enforcement officers conducted searches of NN's room and belongings. In 2005, police searched NN's room in Division 63. A hidden computer was found containing a great amount of child porn. In 2009, September 13, NN was transferred to another ward and in 2010, a police search was carried out again at this location and storage medias were found containing child porn. In summer 2011, rumors from other staff gave away that NN was smuggling forbidden items into his room, and another search was conducted, where they found USB flash drives. Given past actions by NN, and his behavioral history, suspicion arose that these USB sticks would contain some form of child pornographic material [103].

Law

Regarding the law and what rights NN had, confidentiality of a patient only applies when considering health conditions and similar matters. Since NN's behavior could be a result of his condition, this confidentiality should be in effect. Although, there is an exception to most laws, in our case, based on NN's history, there was good reason to breach his confidentiality if there was enough suspicion of a crime against minors (Chapter 3, 4 or 6 of the Criminal Code). Regarding the right

to confiscate the USB sticks without verifying first what was contained in them, the staff was previously notified that NN was handling such material and, according to section 21 of the psychiatric compulsory act, any possession of property that can harm a person can be confiscated and disposed of, given the staff members the right to have taken NN's belongings without warning [103].

SOUTH KOREA

A. Judicial system

The judicial system of South Korea is based on civic law.

Canada vs South Korea judicial system

The judicial system consists of Supreme Court of Korea at the top, Constitutional court,6 high courts, 13 districts Courts and special Jurisdiction Courts such as Family Courts, Municipal Courts.

This can be related to Canada where Supreme Court is the top tier and rest follows, but Canada has common law and South Korea follows civil law. This means in common laws, judges have an active role in developing the laws whereas civil law is based on fixed laws and statuses. Hence common law is more flexible and dynamical.

The major difference from Canada is that South Korea doesn't have the concept of juries and judges make the most of the decisions, whereas in Canada, there is an option to take judge only or jury trials. Although in 2008, South Korea started to experiment with jury trials. [115][116]

Government Type

Canada has a parliamentary democracy, federation, and a constitutional monarchy, whereas South Korea is a republic country.

Law Enforcement

The Korean National Police is the national police department of South Korea, just like Canada has RCMP. Its run under Ministry of Government Administration and Home Affairs. The local police organizations come under NPA. There are seventeen police agencies under. The size of the National police was 106,898 in 2015.Whereas, RCMP had 28,461 personnel in 2015.[117]

B. Cybercrime Laws of South Korea-

Criminal Laws

1. Article 141 (Invalidity of Public Documents, etc. and Destruction of Public goods)

A person who damages or conceals document, other goods or special media records such as electromagnetic record, etc., used by public offices or spoils its utility by other methods, shall be punished by imprisonment by prison labor for not more than 7 years or by a fine not exceeding 10 million won.

2. Article 227-2 (False Preparation or Alteration of Public Electromagnetic Records)

A person with the intention of disrupting business falsely or alters electromagnetic documents or public office shall be punished by imprisonment with prison labor not more than 10 years.

3. Article 232-2(Falsifications or Alteration of Private Electromagnetic Records)

A person who falsifies or alters, with the intention of making any error in the management of affairs, any special media records, such as another person's electromagnetic records concerning any years, shall be punished by imprisonment with prison labor for not more than 5 years, or a fine not exceeding 10 million won.

4. Article 316 (Violation of Secrecy)

A person who opens a sealed or other secretly composed letter, document, or drawing shall be punished by imprisonment with or without labor for not more than three years or with a fine exceeding not more than 5 million won.

5. Article 347-2 (Fraud by the use of Computer, etc.)

Any person who acquires any benefits to property or has a third person acquiring them, by making any data processed after inputting a false information or improper order, or inputting or altering the data without any authority into a data processor shall be punished by imprisonment with prison labor for not more than 10 years, or a fine not exceeding 20 million won.

6. Article 366 (Destruction and damaging of property, data, etc.)

A person who by destroying, damaging or concealing another's property document or special media records, such as electromagnetic records, etc. or by any other means, reduces their utility, shall be punished by imprisonment with prison labor for not more than 3 years or a fine of not more than 7 million won.

7. Article 314 (Interference with Business)

Any person who interferes with another person's business by damaging or destroying any data processor, such as computer, or special media records, such as electromagnetic records, or inputting false information or improper order into the data processor, or making any impediment in processing any data by other way shall be punished by imprisonment for not more than five years or by a fine not exceeding fifteen million won.

8. Article 140 (Rendering Null and Void Symbol of Official Secrecy)

A person who damages or conceals a seal or symbol of attachment or other execution which a public official has levied in his official duties or reduces its utility by any other methods, shall be punished by imprisonment for not more than five years or by a fine not exceeding seven million won.

Act on promotion on information and communications Network Utilisation and Information Protection, etc.

Chapter VI Stability of the information and Communications Network

Article 48

Anyone is prohibited from infiltrating into information and communication network without any justifying access right or his/her permitted access right)

(1) Any person shall be prohibited from transmitting or distributing any program referred to as 'malicious program' that may damage, destroy the information and communication system, alter and forge the data or program, etc. or hinder the operation thereof without any justifiable reasons.

(2) Any person shall be from sending a large volume of signals or data for the purpose of hindering the stable operations of information and communications networks using the methods of getting instructions processed.

Article 49(Protection of Secrets, etc.)

Any person shall be prohibited from damaging the information of other persons or from infringing, stealing or leaking the secrets of other persons, which are processed, stored or transmitted by information and communications networks [9].

Article 61(Penal Provisions)

(1) Any person who has defamed any other person by alleging openly facts through information and communications network with the purpose of slandering him/her shall be punished by imprisonment with or without prison labor for not more than 3 years or by a fine not exceeding 20 million won.

(2) Any person who has defamed any other person by alleging openly false facts through information and communications network with the purpose of slandering him/her shall be punished by imprisonment with prison labor for not more than 7 years or the suspension of disqualification for not more than 10 years, or by a fine not exceeding 50 million won.

Article 62(Penal Provision)

Any person falling under any of the following subparagraphs shall be punished by imprisonment with prison labor for not more than 5 years or by a fine not exceeding 50 million won.

(1) A person who has utilized the personal information or provided it to any third person beyond the scope of the notification or the limit specified in a standardized contract under Article 22 (2) in contravention of Article 24 (1) (including a case where the provisions are applied mutatis mutandis in Article 58).

(2) A person who has utilized the personal information of users for other purpose than the purpose for which such personal information has been provided or provided such personal information to any other person in contravention of Article 24 (2) (including a case where the provisions are applied mutatis mutandis in Article 58).

(3) A person who has damaged, infringed or leaked the personal information of users in contravention of Article 24 (4) (including a case where the provisions are applied mutatis mutandis in Article 58).

(4) A person who has transmitted or distributed malicious programs in contravention of Article 48 (2).

(5) A person who has caused troubles in information and communications networks in contravention of Article 48 (3).

(6) A person who has damaged the information of any other person, or infringed, stolen or leaked the secrets of any other person in contravention of Article 49.

Article 63(Penal Provisions)

Any person falling under any of the following subparagraphs shall be punished by imprisonment with the prison labor for not more than 3 years or by a fine not exceeding 30 million won.

(1) A person who has infiltrated information and communications networks in contravention of Article 48 (1).

(2) A person who has leaked the secrets to any other person, which he/she has learned while performing his duties or utilized such secrets for other purpose than the purpose of his/her duties in contravention of Article 57.

Article 65(Penal Provisions)

Any person falling under any of the following subparagraphs shall be punished by imprisonment with prison labor for not more than 1 year or by a fine not exceeding 10 million won.

(1) A person who has distributed, sold, rented, or openly displayed lascivious codes, letters, sounds, visuals, or films through information and communications networks.

(2) A person who has repeatedly sent words, sounds, letters, visuals, or films inciting fears and uneasiness to any other person through information and communications networks.

Information Infrastructure Protection Act

Article 28

Any person who disrupts, paralyzes, or destroys a Critical Information Infrastructure will be shall be punished by imprisonment with prison labor for not more than 10 year or by a fine not exceeding 100 million won.

C. Cyber Security agencies in South Korea

Korea Internet and Security Agency

It's a subdivision of Ministry of Science and ICT dealing with allocation and maintenance of IPv4 and IPv6 of South Korea and ensuring cybersecurity of South Korea. Cybersecurity is provided by running a CERT (Computer Emergency and Response team), promotion of safe internet usage, detection and analysing malware/virus, privacy protection, etc.

This organisation was created in July 2009 by merger of Korea Information Security Agency, National Internet Development agency and Korean IT International Cooperation Agency.

KRCERT

(Cyber Security Big Data Analysis) This is a centre which aims to analysis threats in cyber world by big data analysis and joint utilisation system by sharing threat information gathered from various institutions, organisations, industries etc. By this, the ability to identify and preventing threats can be strengthened and next generation security measures and equipment can be developed by these analyses.[122]

Cyber Terror Response Center

It's the official division of Korean National Police for cybercrime protection established in 2000.

Cyber Organisation Bureau

This organisation is vigilant on any illegitimate activity on cyber space of Korea such as DDos attacks, hacking, data damage, data leaks, intrusion, etc.

Information Security Measure System (ISMS)

This is a national cybersecurity framework for implementing international recognized cybersecurity standards.

.

D. Cooperation

Interstate cooperation

Korea Internet Security Agency (KISA) has signed with other nation's organisations for implementing cybersecurity, The organisations are listed below:

- Office of Cybersecurity and Information assurance (U.K)
- Israel National Cyber Bureau (Israel)
- Checkpoint (Israel)
- McAfee
- Microsoft
- CERT (Australia)
- CERT(Romania)

- CERT(Japan)
- CERT (China)
- Cyber Security Institute Of Kazakhstan

Intra-Agency cooperation

Korean Government has allowed national and sector specific programs/departments for sharing assets within the public sector through Ministry of Science, ICT and Future Planning.

International cooperation

Korea participates in several cybercrime activities APCERT (Asia Pacific Emergency Response Teams) and is a member [118].

E. Cyber-Crime Incidents and Court Cases in South Korea

1. North Korea attacking South Korean Banks

North Korea attacking South Korean bank (Nonghyup agricultural bank) in 2011. Nearly 30 million customers of Nonghyup agricultural bank were refrained from using online services, ATM and some data was destroyed in April 2011.This was considered most serious attacks on South Korea Conclusively, it was difficult to predict who launched the attack but western analysts who studied the incident agreed that the attack came probably from North Korea and described the first publicly reported case of computer sabotage by one nation against the financial institution of another nation. These types of attacks are relatively cheap to launch but defence is a costly task.

After the incident South Korean bank pledged to spend 476 million dollars in that year on network security.

A researcher from McAfee Labs that analysed the attack stated" North Korea is doing massive damage with simple means. This is Cyberwarfare 101." [104]

Ninety five percent South Koreans have high speed internet access, the highest rate on the planet and extensively use internet for banking, shopping, storing medical records online. So, South Korea can be the biggest target. On the contrary North Korea is an isolated, impoverished state in which only a selected few have access to the internet, fearing the power to spread dissent, restricts its use. With little vulnerability to computer attacks, North Korea is free to focus on offense, which can be low cost and can impact highly.

A laptop used by a subcontractor became a zombie Pc operated by North Korea in 2011, which later remotely staged the attack.

One of the IP address used to break into Nonghyup's system was the same as one used in March for a distributed denial of service(D-dos) attack originated by North Korea. The software used in the attack was also similar to that employed in July 2009, when a number of South Korean government websites were attacked [104].

Laws Violated

Article 141(Invalidity of Public Documents, etc. and Destruction of Public goods)
Punishment- punished by imprisonment by prison labor for not more than 7 years or by a fine not exceeding 10 million won.
Article 232-2(Falsifications or Alteration of Private Electromagnetic Records)
Punishment- punished by imprisonment with prison labor for not more than 5 years, or a fine not exceeding 10 million won.
Article 366(Destruction and damaging of property, data, etc)
Punishment- punished by imprisonment with prison labor for not more than 3 years or a fine of not more than 7 million won.
Article 48(Prohibition to infiltrate in Information System without access)
Punishment- punished by imprisonment with prison labor for not more than 5 years or by a fine not exceeding 50 million won.
Article 28(Information Infrastructure Protection Act)
Punishment- punished by imprisonment with prison labor for not more than 10 year or by a fine not exceeding 100 million won.

2. July 2009 Cyber attack (DDos) (TROJAN DOZER)

In the month of July 2009, there were major attacks on South Korean government, news media, financial websites. The attacks were done with the help of botnets (zombie computers)- a large number of high jacked computers that maliciously attacked targeted websites, overloading their server by influx of large traffic. Almost 200,000 computers were hacked in order to convert them into botnets. At least 39 websites were targeted.

These attacks started the same day as North Korea's ballistic missile test and allegations were made against North Korea regarding the attacks. Lazarus group was attributed for this series of DDos attacks.

Timeline of attacks

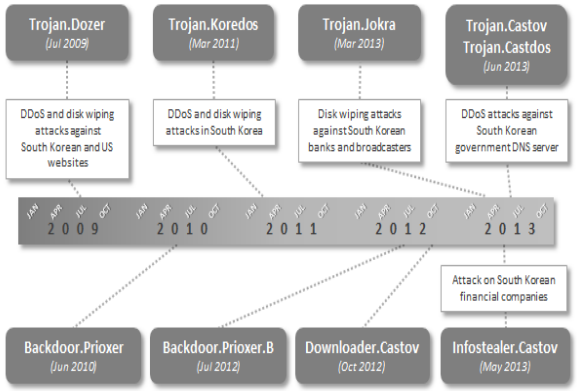
First wave of attack was originated on July 4th, 2009 targeting both South Korea and United States of America. Major

websites like Amazon, White house, New York Stock Exchange, Washington Post etc. were targeted.

Second wave started on July 7th, 2009 effecting Blue house (South Korea president house), the ministry of Defence, the ministry of public administration and security of South Korea, South Korea national intelligence service.
Third wave began on 9th July 2009, attacking Country's National Intelligence Service, as well as large banks, and major news agencies.[105]

Effects

The attacks were performed with the purpose of disruption rather than stealing, South Korea President office stated. However the economic costs associated with the websites being shot down and stopping the services was very large. These were all the Trojan attacks targeted to South Korea illustrated below.



All Trojan attacks on South Korea

Laws Violated

Article 232-2(Falsifications or Alteration of Private Electromagnetic Records)
Punishment- punished by imprisonment with prison labor for not more than 5 years, or a fine not exceeding 10 million won.
Article 366(Destruction and damaging of property, data, etc)
Punishment- punished by imprisonment with prison labor for not more than 3 years or a fine of not more than 7 million won.
Article 48(Prohibition to infiltrate in Information System without access)
Punishment- punished by imprisonment with prison labor for not more than 5 years or by a fine not exceeding 50 million won.
Article 28(Information Infrastructure Protection Act)
Punishment- punished by imprisonment with prison labor for not more than 10 year or by a fine not exceeding 100 million won.

3. South Korea Credit Card breach

There was the biggest credit card breach in the history of South Korea when approximately 104 million credit card accounts were compromised following breaches at three credit card firms.20 million cards were affected during the breaches were reported by BBC in 2014.

Compromised data included the card numbers, names, validation dates, resident registration, birth date, phone number and addresses.
The data breach was done by a person working in Korea Credit Bureau, a firm that produces credit scores. The accused used the company's access to databases containing information on three South Korean credit card firms and copied data onto a USB drive. The person sold all the information and data to various marketing firms. Later, the person was arrested.

The firms affected by this breach are KB Kookmin Card, Lotte Card and NH Nonghyup Card. The firms later reissued the cards to the affected users.

This case is a classic example of an insider threat where an employee (a temporary consultant) accessed and downloaded sensitive data without this being noticed by the company. This kind of breach can become a disaster for a business due to loss of customer confidence or even stealing transactions. [106]

Summary

This was an insider threat which was caused by the misuse of privilege access to the information by an employee, so no big tools are used in these kinds of breaches, just a memory device is enough to store the compromised information.

Laws Violated

Article 227-2(False Preparation or Alteration of Public Electromagnetic Records)
Punishment- Punished by imprisonment with prison labor not more than 10 years.
Article 316(Violation of Secrecy)
Punishment- punished by imprisonment with or without labor for not more than three years or with a fine exceeding not more than 5 million won.
Article 347-2(Fraud by the use of Computer, etc.)
Punishment- punished by imprisonment with prison labor for not more than 10 years, or a fine not exceeding 20 million won.
Article 366- (Destruction and damaging of property, data, etc.)
Punishment- punished by imprisonment with prison labor for not more than 3 years or a fine of not more than 7 million won.

4. Hacking online games (Hacking event)

This event led to the formulation of a new law.

South Korea set up a law in 2017 June on hacking online games in order to cheat. In 2018 January 13 offenders from arcade online game Overwatch were arrested and three of them received the sentences in May 2018. The investigation was a year long journey which began in January 2017.The three sentences are:

- One has received a probation from the government and if he violates, he can end in jail time.
- Second person got fined of 10,000 dollars (10 million Korean won).
- Third person, a 28 years old individual received one year in prison and two years of probation.

One of the hackers generated more than 200 million Korean won (around 180,000 dollars) by hacks. The hacks can range from scripts that aim to match fixing to boost a player's competitive ranking.

Overwatch had a major issue of hacking and cheating during 2016 and 2017 where cheaters can access freebies account after getting blocked. In early 2017, Blizzard (an organisation working with National Police Agency Cyber Security Department), changed the rules for freebie accounts but was not successful in hackers could bypass by hacks.

So, a law was required to target those hackers. Hence 2017 a law was formed which specifically mentions the creation of game hacks as well as the creation and distribution of private servers is punishable under Korean Constitution. [108][109]

Punishment

Those who found guilty in this can face a maximum fine of 50.000 dollars and maximum sentence of not more than 5 years in prison.

5. Court Case Documented

In summer 2015, photos and videos of 200 women in compromising moments were caught by a hidden camera placed in the changing rooms in a waterpark in Yongin. These photos were distributed on the internet.

Investigation- The photos and videos were uploaded on International websites, so was difficult to trace but after an investigation police traced a photograph of a women in a mirror with a cell phone in her hand. This woman was suspected to perform this crime and later was caught by the police. The women in her late twenties was hired by a person to place and record videos of women undressing in return of 1.3 million won.

Trial- On January 14th, 2016, Kang Mo (33) and Choi Mo (26) were arrested for alleged violation of Special Act on the Punishment of Sexual Violence Crimes under the First Court of Justice District Act and were sentenced for four years and three months and three years respectively in prison [112].

III. METHODOLOGY

A. Cyber laws amd incidents comparison tables

The objective of this project is to make a comparison between some of the most representative cybercrime laws of Canada and countries such as Ecuador, Iran, Turkey, Sweden and South Korea.

Canada

Canada will be the basis for this comparison. In this section we detailed the cybercrime laws from Canada and also some incidents or court cases where such laws have been compromised.

Canadian Cyber Crime Laws	
Canadian Law	Related cases
(A) C.C.C. Art. 342.1 - Unauthorized use of a computer	CONCORDIA CASE [126]
(B) C.C.C. Art.162 - Voyeurism	Accused teacher using concealed camera to make surreptitious video recordings of female high school students engaging in ordinary school-related activities in common areas of school. Accused charged with voyeurism [127].
(C) C.C.C Art.342.2 - Possession of device to obtain computer service (hacking tools)	Man arrested for interception of electronic communication and possession of electronic interception devices [128].

(D) C.C.C. Art. 163.1 - Corrupting morals, Production, distribution and possession of child pornography	Graphic sexual images of a female grade ten student were discovered on high school teacher's work issued laptop by a school computer technician assessing system stability concerns on the school network [129].
(E) C.C.C. Art.430(1.1) Mischief to data	Wajam Internet Technologies Inc. breaches multiple provisions of PIPEDA (Personal Information Protection and Electronic Documents Act) [130].
(F) C.C.C Art.184 - Illegal interception of a private communication	Illegal recording of private conversation gets thrown out in court [131].
(G) C.C.C. Art.326 - Theft of telecommunication	Companies in Canada were among the targets of two Chinese citizens charged with waging an extensive hacking campaign to steal valuable data over many years by using telecommunication [132].
(H) C.C.C. Art.42 - Offences related to copyrighted property	The person is facing legal actions in Federal Court launched by a prestigious Toronto law firm on behalf of U.S. movie production companies attempting to enforce their copyright claims [133].
(I) C.C.C. Art. 172.1 – Luring a child	A man who was convicted of luring a 14-year-old girl who turned out to be an undercover police officer [134].
(J) C.C.C. Art. 342 – Theft, forgery, etc., of credit card	Leaked Data reveals hackers have private credit card information of over 100 million individuals using Capital One financial organization [135].
(K) C.C.C. Art. 354 – Possessing of data, password, lists, etc. criminally obtained	Trafficking in Identity Information and Possession of Property. The company pleaded guilty to the charges of Trafficking in Identity Information and Possession of Property Obtained by Crime [136].
(L) C.C.C. Art. 380 - Frauds	PacNet Services Ltd employees were charged with engaging in a massive fraud scheme in which their company processed payments from victims of numerous international mass-mail fraud campaigns [137].

Canada and Ecuador comparison

Comparison between Canada and Ecuador Cybercrime Laws		
Canadian Law	Ecuadorian Law	Related cases in Ecuador
A	COIP Art. 234 - Unauthorized access to a computer, telematic or telecommunications system	ECUADOR – CASE 1 Hackers gain unauthorized access to the computer system of the University "Espíritu Santo" to change students' grades. [42]
B	-	-
C	COIP Art. 230 (4) - Illegal interception of data	ECUADOR - CASE 2

D	COIP Art. 103 - Pornography involving children or adolescents	INTERPOL in coordination with some Latin American countries, undertook an operation to capture criminals using online forums to share and distribute child sexual abuse materials. [43] The Attorney General's Office of Ecuador demonstrated the crime of child pornography of a citizen who used social networks to exchange illegal content. [44]
E	COIP Art. 232 - Attack on the integrity of computer systems	A Swedish citizen was arrested in Ecuador for alleged participation in the crime of attacking the integrity of computer systems. [45] Extensive malware, phishing, and disinformation campaign active in several Latin American countries, some political interests may be involved. [46]
F	COIP Art. 230 (1) - Illegal interception of data	Different cases of electronic data interception in Ecuador. What laws in the Criminal Code punish this type of crime? [47]
G	COIP Art. 190 - Fraudulent appropriation by electronic means	Losses of around 200 million dollars per year are calculated by the Ministry of Electricity and Non-Renewable Energies of Ecuador. [48]
H	Law on Intellectual Property - Chapter III	The National Service of Intellectual Rights carried out an operation to block IP's that allowed access to unauthorized television content. [49] The piracy of CDs (music, movies, software, etc.) is one of the most common copyright crimes, but it is still a difficult issue for prosecutors to fight. [50]
I	COIP Art. 173 - Sexual contact with minors under the age of eighteen by electronic means	ECUADOR - CASE 3
J	COIP Art. 230 (3) - Illegal interception of data	ECUADOR - CASE 2
K	COIP Art. 178 - Violation of privacy	A blogger was arrested for obtaining personal data of the president of Ecuador, from a database of the "Dato Seguro" informatic system. [51] The organization “Usuarios Digitales”, reported the theft of information from a database of “Escuala de la Función Judicial”, after massive attacks by hackers. [52]
L	COIP Art. 186 - Fraud	“Banco del Austro” loses $12 million via SWIFT fraudulent transactions. [53]

Ecuador analysis

When talking about cybercrime in Canada, it is important to mention that in 2001, the year in which the Budapest Convention of Cybercrime was held, Canada agreed to sign this international treaty [138], which encouraged cooperation among nations and the implementation of new laws to combat this type of crime more effectively.

In the case of Ecuador, the problematic of cybercrime is relatively new. It was not until 2014 that, following a process of restructuring the Ecuadorian constitution, it was decided to incorporate certain laws into the new Criminal Code in order to combat these types of cybercrimes. Before 2014, Ecuador had the Law of Electronic Commerce, Digital Signatures and Data Messages, which was included in 2002, however, the

spectrum covered by this law is very limited and it only contemplates certain rules on cybersecurity in the country.

After carrying out the present project, it was possible to identify the following differences related to cybercrime between Canada and Ecuador

- One of the major differences between these two countries is that the Ecuadorian law against cybercrime still needs to mature and "it is necessary to promote the generation of a global culture of cybersecurity in the country." [139]. In contrary, Canada has a well-defined judicial and legal system to fight against these types of crimes.
- Ecuador has not defined a National Cybersecurity Plan, unlike Canada, which has a National Cyber Security Strategy, a document that outlines how to both prevent cybercrimes and combat them when they occur.
- As for the laws related to cybercrime, specifically for the Canadian law C.C.C. Art. 162 (1) - Voyeurism, no equivalent could be found in the Ecuadorian Criminal Code (COIP). However, it could be related to article 178 - Violation of privacy of the COIP, which states "Any person who, without the consent or legal authorization, accesses, intercepts, examines, retains, records, reproduces, disseminates or publishes personal data, data messages, voice, audio and video, postal objects, information contained in computer media, private or confidential communications of another person by any means, shall be liable to a term of imprisonment of one to three years".[12]
- Ecuador is not yet a member of the Budapest Convention of Cybercrime, which directly affects the country in terms of international cooperation for the exchange of information and joint operations related to cybercrime. However, Canada did so in 2001 and since then has benefited from the advantages of being part of this international treaty.

Canada and Iran comparison

Comparison Between Canada and Iran Cyber Crime laws		
Canadian Law	**Iran's Related Laws**	**Related Cases**
A	ICCA Art.1 (Unauthorized Access), Art.3 (Unauthorized interception), Art.4 (Computer Spy)	Iran – Case 1 DDoS attack against online payment websites [37]
B	ICCA Art.16-17-18 (Aspersion of Dignity and Issuing Lies)	Capturing the blackmailer who threaten to release private images of victim [40]
C	ICCA Art.25 (Miscellaneous Crimes)	Iran - CASE 2 Installing keylogger spyware on victim's devices by publishing it in the social media or by sending an infected email in the format of photo, music, software. [38]
D	ICCA Art.14 (Crimes against Public Morality and Chastity)	Publication of child rape videos on the internet and arrest of rapist and publisher [41]
E	ICCA Art.3 (Computer Spy), Art4 (Computer Spy), Art.6 (Computer Forgery counterfeiting), Art.8 (Data or Computer or Telecommunication Systems interference), Art.9 (Data or Computer or Telecommunication Systems interference)	Iran- Case 1 DDoS attack against online payment websites [37]
F	ICCA Art.2 (Unauthorized interception), Art.48(Interception the Content data)	Iran-Case 3 Tricking people into installing unauthorized applications and then defrauded them. [39]
G	ICCA Art.3(Unauthorized interception), Art.4(Computer Spy), Art.6(Computer Forgery counterfeiting), Art.8(Data or	Iran-Case 3 Tricking people into installing unauthorized applications and then defrauded them. [39]

	Computer or Telecommunication Systems interference)	
H	Intellectual property law Art.12	There is no proper law for copyright in Iran in cyber space.
I	ICCA Art.14(Crimes against Public Morality and Chastity)	Publication of child rape videos on the internet and arrest of rapist and publisher [41]
J	ICCA Art.7(Crimes against Integrity and validity of Data and Computer and Telecommunication Systems), Art.6(Computer Forgery counterfeiting), Art.13(Computer Related Theft and Fraud)	Iran - CASE 2 Installing keylogger spyware on victim's devices by publishing it in the social media or by sending an infected email in the format of photo, music, software. [38]
K	ICCA Art.12(Computer Related Theft and Fraud), Art.28	Iran - CASE 2 Installing keylogger spyware on victim's devices by publishing it in the social media or by sending an infected email in the format of photo, music, software. [38]
L	ICCA Art12, Art.13(Computer Related Theft and Fraud)	Iran-Case 3 Tricking people into installing unauthorized applications and then defrauded them. [39]

Iran analysis

According to the information provided in this study, as it has been observed, Iran has numerous laws related to cybercrime, and laws are being updated on a daily basis according to world standards and events. The biggest difference between Iranian and Canadian cyber laws is that Iran has combined Islamic law with cybercrime laws in some areas, including pornography, Insults to individuals and blasphemy.
The Copyright Act hasn't evolved in Iran yet, and it's only applied to domestic products within the country.
A comprehensive illustration of cyber-criminal law in Iran may be useful for comparative studies among Islamic and non-Islamic systems.

Criminal justice has made some important progress in tackling cybercrimes in Iran. Legislator has addressed regulatory needs of cyberspace both in general policies and ordinary legislations, most important of which is Cyber Crime Act passed in 2009. Electronic Commerce Act is another important enactment. However, the legal infrastructures of cyberspace are still in progress in Iran and several projects are being conducted under the supervision of Ministry of ICT.

Cyber Crime Act is inspired mainly by Cyber Crime Convention of European Council 2001. Notwithstanding, criminal laws related to the criminal contents are based upon Islamic criminal laws. The Act has listed main cybercrimes and provided differentiated and special criminal procedure for prosecution of these crimes. The law has also established special criminal justice institutions such as cyber police, cyber prosecutorial office and courts for cyber-crimes. However, in spite of all these progresses there are still some deficiencies which need to be addressed in future. Some of these deficiencies are as follows:

- Some forms of harmful conducts are not criminalized, conducts like: identity theft, spam and cyber money laundering…
- Vagueness in cyber evidence rules and investigation procedures,
- Unclear rules of jurisdiction,
- Some deficiencies of the evidences and documentation of electronic evidences,
- Cyber Crime Act has delegated the power of law making to state in some respects for which the Parliament is the only competent authority according to the Constitution.

The lack of a system for international cooperation in combating cyber-crimes, this problem is not however special to this Act. In international level the question of cooperation in cyber criminality is also a challenging matter and remains on United Nation and other international organizations to set up a global system for preventing and combating this form of criminality.

Canada and Turkey Comparison

Comparison Between Canada and Turkey Cyber Crime Laws		
Canadian Law	Turkey's Related Laws	Related Cases
A	Turkish Law no. 5237 - 243 (Accessing a data processing system)	Turkey Case 1 Hacking and publicizing the emails of the Minister of Energy and Natural Resources Turkey Case 2 Being member of the leftist hacker group RedHack and being part of cyber attack on the Ankara Police Department
B	Turkish Law no. 5237 - 134 (Privacy of private life)	Turkey Case 6 Committing voyeurism crime by using hidden cameras in the toilet, blackmailing employees, and having inappropriate images of children
C	Turkish Law no. 5846 - 72 (Intellectual and Artistic Works)	Turkey Case 2 Being member of the leftist hacker group RedHack and being part of cyber attack on the Ankara Police Department
D	Turkish Law no. 5237 - 226 (Obscenity)	Turkey Case 4 Downloading, saving, and sharing child pornography Turkey Case 6 Committing voyeurism crime by using hidden cameras in the toilet, blackmailing employees, and having inappropriate images of children
E	Turkish Law no. 5237 - 243 (Accessing a data processing system) Turkish Law no. 5237 - 244 (Preventing the functioning of a system and deletion, alteration, or corrupting of data)	Turkey Case 1 Hacking and publicizing the emails of the Minister of Energy and Natural Resources Turkey Case 2 Being member of the leftist hacker group RedHack and being part of cyber attack on the Ankara Police Department Turkey Case 3 Hacking the Ministry of Education`s grading and attendance system
F	Turkish Law no. 5237 - 243 (Accessing a data processing system)	Turkey Case 1 Hacking and publicizing the emails of the Minister of Energy and Natural Resources Turkey Case 2 Being member of the leftist hacker group RedHack and being part of cyber attack on the Ankara Police Department Turkey Case 3 Hacking the Ministry of Education`s grading and attendance system
G	Turkish Law no. 5651 - 6.1 (Accessing Provider)	No Case Identified
H	Turkish Law no. 5846 - 71 (Intellectual and Artistic Works) Turkish Law no. 5846 - 72 (Intellectual and Artistic Works) Turkish Law no. 5846 - 73 (Intellectual and Artistic Works) Turkish Law no. 5846 - 75 (Intellectual and Artistic Works)	No Case Identified

I	Turkish Law no. 5237 -103 (Child Sexual Abuse)	Turkey Case 4 Downloading, saving, and sharing child pornography Turkey Case 6 Committing voyeurism crime by using hidden cameras in the toilet, blackmailing employees, and having inappropriate images of children
J	Turkish Law no. 5237 – 245 (Misuse of bank or credit cards)	Turkey Case 1 Hacking and publicizing the emails of the Minister of Energy and Natural Resources Turkey Case 2 Being member of the leftist hacker group RedHack and being part of cyber attack on the Ankara Police Department
K	Turkish Law no. 5651 - 6.1 (Accessing Provider)	Turkey Case 2 Being member of the leftist hacker group RedHack and being part of cyber attack on the Ankara Police Department
L	Turkish Law no. 5237 - 158.1 (Corresponding article in the legislation) Turkish Law no. 5237 - 243.2 (Accessing a data processing system)	Turkey Case 5 Operating a phishing website that impersonated bank site, tricking victims into providing their bank details Turkey Case 6 Committing voyeurism crime by using hidden cameras in the toilet, blackmailing employees, and having inappropriate images of children

Turkey Analysis

Canada and Turkey have slight differences to each other in terms of laws and incidents. Canada is based on English common law, except in Quebec where a civil law system based on French law. Turkey is based on Swiss civil law. Also, Turkish law is under influence of secularism so that law is not mixed with religious law.

Cyber-crimes were first introduced to the Turkish Penal system on 6 June 1991 with Law No. 3756 targeting several amendments to the Turkish Penal Code. After that the government of Turkey started to legislate new laws against to cyber-crimes.

According to the project about cybercrime laws, major comparisons between Turkey and Canada are observed below:

- There is no law in Turkey under name of Voyeurism. When a crime about Voyeurism occurs, the trial charges a person under the law of Privacy of Private Life (Turkish Law no. 5237 – 134).
- There is no specific law or regulation regarding access to encrypted data in Turkey
- There are no specific laws or policies on technology neutrality in Turkey
- There is no relevant law about data breach notification in Turkey
- Turkey is a member of the WTO, but not a member of the WTO (World Trade Organization) plurilateral Agreement on Government Procurement unlike Canada [140]
- Internet censorship is common in Turkey, and sites can be blocked for several reasons. Under the Law on the Internet (No. 5651/2007). The government of Turkey has right to block any website that is considered as illegal
- Turkey signed the Council of Europe Convention on Cybercrime in 2010. However, the full range of offences in the Cybercrime Convention have not yet been implemented in Turkish domestic law. The key outstanding requirement is that Turkey does not yet have an offence relating to `misuse of devices` as required by Article 6 of the Cybercrime Convention [141]
- Turkish criminal law includes extra-territorial application to Turkish citizens. Turkey is also a member of the Cybercrime Convention and will cooperate with law enforcement agencies in other jurisdictions in the investigation of cybercrimes [141]
- Turkey has a moderate level of protection available for cloud services, through a combination of its cybercrime legislation and copyright laws. However, both laws have minor gaps, and Turkey

does not yet have data protection legislation in place [141]

Canada and Sweden Comparison

Comparison between Canada and Sweden Cybercrime Laws		
Canadian Law	Sweden Law	Related cases in Sweden
A	Chap 4 S 9c – Unauthorized Access to data	School Computers Hacked. [142] Swedish schoolkids hack computers to change grades, fend off alerts to parents
B	Chap 4 S 7 – Exposing Disturbing Material	Recording of Intimate Interaction (2)
C	Chap 8 S 12 – Preparation to Commit a Crime	
D	Chap 16 S 10a – Possession of Child Pornography	Patient convicted with possession of child porn (3)
E	Chap 4 S 9c – Unlawful access or alteration to data	Twitter Account Hacked[143] Swedish Social Democrats' Twitter account hacked Overnight
F	Chap 4 S 8 – Unlawful access to communication	Train Delays[144] DDoS Attacks Cause Train Delays Across Sweden
G	Chap 4 S 9 – Telecommunication Theft	Hotline Blocked[145] Hotline Riot from 1982
H	(1960: 729) Copyright Act for literary and artistic works	Pirate Bay Trial (1)
I	Chap 16 S 12 – Corrupting Children	Doctor Child Sex Abuse[146] Spanish doctor charged with child sex abuse in Sweden
J	Chap 8 S1 – Theft	Credit Card Fraud[147] Report on card fraud, Sweden and credit card fraud
K	Chap 9 S 6 – Possession of Criminally obtained Material	User Data Breach[148] Swedish Crypto Exchange QuickBit Announces User Data Breach
L	Chap 9 S 1 – Fraud	Instagram Fraud[149] New Cryptocurrency Wave of Fraud Hits Instagram In Sweden

Sweden Analysis

According to the Swedish Penal Code [93], criminal offences such as hacking, denial-of-service attacks and phishing are considered data breaches. The possession of hacking tools is not criminalized in Sweden but is deemed a criminal offense in case of preparation for a data breach [150]. The crime punishment is a fine or a prison term of up to two years. Preparing for a severe infringement of information is punishable by imprisonment for at least six months but not more than six years [93].

Regarding the applicable law in cybersecurity, the EU General Data Protection Regulation (GDPR) regulates the processing of personal data [151]. The Swedish Act on Processing of Personal Data Relating to Criminal Offences regulates the processing of data by governmental agencies relating to investigation, prevention and prosecution [93]. As shown in the table above, criminal offences are subject to the Penal Code. The Swedish Copyright Act prevents the use, creation, advertising and ownership of technical tools, parts and facilities aimed at gaining unauthorized entry to copyrighted content [151].

Sweden bases its modern criminal prosecutions on old laws presented in the Penal Code, the most appropriate and relatable Acts will apply, along with the appropriate punishment that may or may not come from the punishments stated in the Penal Code depending on how serious the crime is. For instance, destroying the data of computers can be considered 'damage to property' in the Penal Code, and if the act was performed on devices belonging to national security, the act can be considered 'sabotage' in the Penal Code.

Canada and South Korea Comparison

Canada vs South Korea Cybercrime laws		
	South Korea	
Canadian Law	**Laws**	**Cases**
A	Article 347-2"Frauds related to computers", Network Act,	Hacking Case-The hackers used illegal scripts for the purpose of cheating and generating large amount of money illegally in the game Overwatch. [108][109]
B	Article 14"Act of special cases concerning the punishment, etc of sexual crimes	Compromising photos of 200 women in changing rooms were captured with hidden cameras and shared.[112]
C	Network Act	Hacking Case-The hackers used illegal scripts for the purpose of cheating and generating large amount of money illegally in the game Overwatch.[108][109]
D	Article 243, Article 244	A man was caught running paid membership child pornographic website with 100 million members.[110]
E	Article 314"Interference with Business", Article 366"Destruction and Damage, etc. of Data"	Credit Card Breach-AN insider of the company got illegal access to the credit card database and stole the data and sold it to advertising companies.[106][107]
F	Protection of communication secrets act.	No incident found
G	Act of Promotion of Information and Communication Network Utilization and Information Protection	Spam and phishing on rise, resulting the government to block the illegal telephone numbers.[123]
H	Copyright Act	Four martial arts novels such as Mr. A sued police for not taking proper steps for the copyright cases they filed.[111]
I	Article 242"Arranging for prostitution", Article 302"Sexual Intercourse with minors", Article 305"Indecent act with minors",	Three men raped three female students, took photos and shared them prisoned for three years.[113]
J	Electronic Financial Transaction Act, Use and protection of credit card act	Credit Card Breach-AN insider of the company got illegal access to the credit card database and stole the data and sold it to advertising companies.[106][107]
K	Article 316"Violation of Secrecy"	Trojan Dozer-unsuspected DDOS attacks were performed on South Korean government, banks etc with the help of botnets. Suspected group was Lazarus group.[105] North Korea attacking South Korean banks-North Korea hackers were suspected to perform Ddos attacks on South Korean banks in 2011 blocking the bank servers and delaying transactions.[104]

L	Article 347"Frauds"	1). Hacking Case-The hackers used illegal scripts for the purpose of cheating and generating large amount of money illegally in the game Overwatch. [108][109] 2). Credit Card Breach-AN insider of the company got illegal access to the credit card database and stole the data and sold it to advertising companies.[106][107]

South Korea Analysis

South Korea has not signed in The Convention of Cybercrime treaty which was held in Budapest in 2001, which encourages co-operation of European Nations as well as some American and Asian nations to combat cybercrime, where Canada was a part, but South Korea actively participates in APCERT (Asia Pacific Computer Emergency Response Teams). Around 95.1 % population of South Korea has access to internet and is ranked 16th globally, which is more compared to 89 % Canadian population accessing internet. Hence, due to the amount of people using internet, advanced IT infrastructure and an active rival North Korea, South Korea can become the prime target for Cyber-attacks.

During the past 10 years South Korea had observed much more Trojans/DDos and damaging attacks on financial organizations as compared to Canada. Korea has an advanced National Cyber Crime Center like Canada helping in combating with cybercrimes and cyber terrorists and a well-supported connection between the local as well as state government. South Korea is the first democratic country which has passed cyber defamation Law where the Korean police has been given the power to crack down hate comments without the victim's complaint. It's also observed that due to other nations or cybercrime syndicates attacking South Korean information infrastructure, South Korea has a special law dedicated to the same, where any person attacking a critical information infrastructure is sentence with harsh punishments.

South Korea follows civil law whereas Canada follows common law. In common laws, judges have an active role in developing the laws whereas civil law is based on fixed laws and statuses. Hence common law is more flexible and dynamical. South Korea is relatively new in jury trials as compared to Canada where jury trials are relatively old.

IV. Conclusions

Information technology has profoundly affected all aspects of social life, culture, and even criminal laws. The dependencies of modern life on cyber technology.

The nature of these crimes and the abuses committed in this new virtual space has never been seen in the real world. The inadequate security of technology along with its virtual nature provides the opportunity for malicious people. The most worrying aspect of cyberspace is the rapid dissemination of information in it, for example, in a matter of seconds a piece of information that can be potentially exploited is discovered. In cyberspace, it is more difficult to find and fight these crimes.

The "anarchic" status of cyberspace has profound implications for national interests and national security. Many anonymous actors threaten other actors' interests and critical infrastructure daily. Governments need to find a way to mitigate the damage done to these assets.

With the advent of the smart age, the prevailing prediction is that Internet crime and security threats will increase more and more. Budapest Treaty is the first international cybercrime prosecution treaty with detailed laws on cybercrime. Except for European countries, the United States, Canada, and Japan have also joined the treaty. South Korea has also been considering to be a member to the Budapest treaty through the State Department, the Ministry of Justice and the National Police for several years but hasn't come to a conclusion yet.

If there is an international cybercrime incident, there may be many questions about the criminal jurisdiction of the crime. The most effective way to solve this problem is to create a unifying principle in the field of global cybercrime under international law. Implementing such a principle still seems difficult.

As mentioned above, international cybercrime happens in cyberspace regardless of location and time. Under these circumstances, even if there is an international treaty on the criminal jurisdiction of international cybercrime, it would be in vain if all the countries of the world did not participate on it. It is true that the information revolution through computers and the Internet has made a huge contribution to human development, and no one can deny this fact. Since it is possible to move information across borders, cultural exchanges and diplomatic exchanges have been taking place actively across borders, and these international collaborations have been covered by a new paradigm called globalization.

However, like borderless information exchange and interaction, it has become easier to jump from border controls to commit cybercrimes. Unlike developed countries, which

are the biggest beneficiaries of the information revolution, the legal systems of developing countries that are relatively less favored, are technically underdeveloped. So, they are in a position where they can barely deal with new cybercrimes.

As a result, cybercrime has caused worldwide financial damage, but humanity has not been able to effectively control it. However, humanity is experiencing the development of innovative information and technology, and the dimensions of cybercrime that are being exploited by this process are increasing day by day.

Cybercrime is committed regardless of geographical or pre-planned boundaries. Therefore, international cooperation is defined based on punishment for criminals and international standards. In order to increase national capacities, joining to the Budapest Convention on Cybercrime should be implemented as soon as possible for the countries that are not part of it.

REFERENCES

[1] P. Grabosky, "The 2 evolution of cybercrime," *Cybercrime through an Interdisciplinary Lens*, pp. 15, 2016.

[2] Government of Canada. *The judicial structure*. [Online]. Available: https://www.justice.gc.ca/eng/csj-sjc/just/07.html

[3] Wikipedia. *Canada*. [Online]. Available: https://en.wikipedia.org/wiki/Canada

[4] Canada Guide. *The Canadian Legal System*. [Online]. Available: http://www.thecanadaguide.com/basics/legal-system/

[5] Royal Canadian Mounted Police. *Federal Policing Service*. [Onine]. Available: http://www.rcmp-grc.gc.ca/on/prog-serv/index-eng.htm

[6] Royal Canadian Mounted Police. *Royal Canadian Mounted Police Cybercrime Strategy*. [Online]. Available: http://www.rcmp-grc.gc.ca/en/royal-canadian-mounted-police-cybercrime-strategy

[7] Government of Canada. *Justice Law Website*. [Online]. Available: https://laws-lois.justice.gc.ca/eng/acts/C-46/index.html

[8] Government of Canada. *Global Affairs Canada*. [Online]. Available: https://www.international.gc.ca/crime/cyber_crime-criminalite.aspx?lang=eng

[9] Government of Canada. *Cybercrime*. [Online]. Available: https://www.canada.ca/en/services/policing/police/crime-and-crime-prevention/cybercrime.html

[10] M. D. Miño. *UPDATE: The Basic Structure of the Ecuadorian Legal System and Legal Research*. [Online]. Available: https://www.nyulawglobal.org/globalex/Ecuador1.html.

[11] Organization of American States. *Information Exchange Network for Mutual Assistance in Criminal Matter and Extradition*. [Online]. Available: https://www.oas.org/juridico/mla/sp/ecu/.

[12] R. Oficial, "Código Orgánico Integral Penal," 2014.

[13] N. J. Ortiz Campos. *Normativa Legal sobre Delitos Informáticos en Ecuador*. Revista Científica Hallazgos21, 4(1), 100-111. [Online]. Available: https://revistas.pucese.edu.ec/hallazgos21/article/view/336

[14] Unión de Naciones Suramericanas. *Consejo de Defensa Suramericano de UNASUR*. [Online]. Available: http://www.unasursg.org/es/consejo-defensa-suramericano-unasur

[15] Forum of Incident Response and Security Teams. *About FIRST*. [Online]. Available: https://www.first.org/about/

[16] M. Flores and F. Stephanía, *Desafíos De La Ciberseguridad y Respuestas Estatales: El Caso Del Estado Ecuatoriano En El Período 2008-2015.*, 2017.

[17] Chief of Staff, Cyber Defense Command of Ecuador (F. S. Flores, Interviewer)

[18] Policia Nacional del Ecuador. *Misión/Visión*. [Online]. Available: https://www.policiaecuador.gob.ec/mision/

[19] Policia Judicial. *Misión*. [Online]. Available: https://www.policiaecuador.gob.ec/dnpj/

[20] EcuCERT. *Nosotros*. [Online]. Available: https://www.ecucert.gob.ec/nosotros.html

[21] Centro de Inteligencia Estratégica. *Misión y Visión*. [Online]. Available: https://www.cies.gob.ec/archivos/4572

[22] Fiscalía General del Estado. *Diez ciudadanos con prisión preventiva por asociación ilícita en caso 'Impacto Inicial'*. [Online]. Available: https://www.fiscalia.gob.ec/diez-ciudadanos-con-prision-preventiva-por-asociacion-ilicita-en-caso-impacto-inicial/

[23] Fiscalía General del Estado. *Seis sentenciados a 12 meses de prisión en el caso 'Skimmer Uno'*. [Online]. Available: https://www.fiscalia.gob.ec/seis-sentenciados-a-12-meses-de-prision-en-el-caso-skimmer-uno/

[24] El Telégrafo. *6 personas recibieron sentencia tras admitir delito*. [Online]. Available: https://www.eltelegrafo.com.ec/noticias/judicial/12/6-personas-recibieron-sentencia-tras-admitir-delito

[25] Teleamazonas. *Un hombre fue detenido por delito cibernético con fines sexuales en Baños*. [Online]. Available: http://www.teleamazonas.com/2019/03/un-hombre-fue-detenido-por-delito-cibernetico-con-fines-sexuales-en-banos/

[26] Q. Rodríguez and D. Acacio, *Las Políticas Regionales Sobre Ataques Informáticos y Su Incidencia En La Vulnerabilidad De La Defensa De La UNASUR En El Período 2009-2013*, 2014.

[27] La Hora. *4 sentenciados en caso de títulos falsos*. [Online]. Available: https://lahora.com.ec/noticia/1101927597/4-sentenciados-en-caso-de-tc3adtulos-falsos

[28] "Re-emergence of an energy giant", [Online]. Available: https://www.skuld.com/topics/port/port-news/asia/spotlight-on-iran/

[29] Mahdieh Zare, An Overview of Iranian Legal System", [Online]. Available: https://www.nyulawglobal.org/globalex/Iran_Legal_System_Research1.html#IranianLegalSystem

[30] Computer Crimes Act. [Online]. Available: http://cyber.police.ir/index.jsp?pageid=632&p=1

[31] Iranian Cyber police. [Online]. Available: https://www.cyberpolice.ir/#no-back

[32] Organized Crime Investigation Center. [Online]. Available: https://gerdab.ir/fa/content/3

[33] Committee for determining the criminal contents. [Online]. Available: https://internet.ir/

[34] Iranian Ministry of Intelligence. [Online]. Available: http://www.vaja.ir/Portal/Home/

[35] Passive Defense Cyber Division. [Online]. Available: https://papsa.ir/

[36] MAHER CERT. [Online]. Available: https://cert.ir/

[37] "Trace of Iranian Telegram's patches in DDoS Attacks". [Online] Available: http://bit.ly/2YZM5fR

[38] Yasa. A chat with veteran hacker. [Online]. Available: https://www.yasa.co/blog/chat-with-hacker-veteran-2000-bank-accounts-on-the-hacker-list/

[39] YJC. Internet thievery from 300 bank account. [online]. Available: http://bit.ly/33v9wkQ

[40] Asriran. Internet blackmail from the forgetful girl. [Online]. Available: http://bit.ly/2YT7YCA

[41] Tabnak. Publication of child rape videos on the internet and arrest of rapist and publisher. [Online]. Available: https://bit.ly/2KUlwUg

[42] Expreso. *Alumnos de la UEES están preocupados por el hackeo*, 28-Feb-2013. [Online]. Available: https://www.expreso.ec/guayaquil/alumnos-de-la-uees-estan-preocupados-por-el-h-GEGR_4180563

[43] INTERPOL. *Supported operation targeting online child abuse materials leads to arrests across Latin America*, 14-Aug-2013. [Online]. Available: https://www.interpol.int/News-and-Events/News/2013/INTERPOL-supported-operation-targeting-online-child-abuse-materials-leads-to-arrests-across-Latin-America

[44] Fiscalía General del Estado Ecuador. *Fiscalía demostró delito de pornografía infantil y obtuvo sentencia de 17 años y 3 meses*, 24-Jan-2018. [Online]. Available: https://www.fiscalia.gob.ec/fiscalia-demostro-delito-pornografia-infantil-obtuvo-sentencia-17-anos-3-meses/

[45] Fiscalía General del Estado Ecuador. *Ciudadano sueco fue procesado por presunto ataque a la integridad de sistemas informáticos*, 13-Apr-2019. [Online]. Available: https://www.fiscalia.gob.ec/ciudadano-sueco-fue-procesado-por-presunto-ataque-a-la-integridad-de-sistemas-informaticos/

[46] Scott-Railton, J., Marquis-Boire, M., Guarnieri, C. and Marschalek, M. (2015). *Packrat: Seven Years of a South American Threat Actor*, 8-Dec-2015. [Online] The Citizen Lab. Available at: https://citizenlab.ca/2015/12/packrat-report/
[47] El Comercio. *Quien intercepte mensajes puede ser sancionado con 5 años de prisión*, 20-Jul-2015. [Online]. Available: https://www.elcomercio.com/actualidad/interceptar-mensajes-presion-hackeo-ecuador.html
[48] El Universo. *Robo de electricidad deja millonarias pérdidas en Ecuador*, 20-Oct-2009. [Online]. Available: https://www.eluniverso.com/2009/10/20/1/1356/robo-electricidad-deja-millonarias-perdidas-ecuador.html
[49] Servicio Nacional de Derechos de Autor Ecuador. *SENADI dispone el bloqueo de IP's que permitirían el acceso a señales de TV sin autorización*. [Online]. Available: https://www.derechosintelectuales.gob.ec/senadi-dispone-el-bloqueo-de-ips-que-permitirian-el-acceso-a-senales-de-tv-sin-autorizacion/
[50] El Telégrafo. *Delito de propiedad intelectual, un tema difícil para fiscales*, 29-Jun-2013. [Online]. Available: https://www.eltelegrafo.com.ec/noticias/judicial/12/delito-de-propiedad-intelectual-un-tema-dificil-para-fiscales
[51] Peru.com. *Detienen a bloguero por acceder a datos privados de Rafael Correa*, 30-Nov-2012. [Online]. Available: https://peru.com/actualidad/internacionales/ecuador-detienen-bloguero-acceder-datos-privados-rafael-correa-noticia-107210
[52] El Comercio. *'Hackers' lanzaron ofensiva global para atacar web estatales*, 16-Apr-2019. [Online]. Available: https://www.elcomercio.com/actualidad/hackers-ofensiva-global-ataque-ecuador.html
[53] Trend Micro. *Ecuadorean Bank Loses $12 million via SWIFT*, 20-May-2016. [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/ecuadorean-bank-loses-12m-via-swift
[54] S. Bıçak et al., "A Primer on Cyber Security in Turkey and the Case of Nuclear Power," 1 January 2016. [Online]. Available: http://edam.org.tr/en/a-primer-on-cyber-security-in-turkey-and-the-case-of-nuclear-power/.
[55] E. Şeker and İ. B. Tolga, "National Cyber SecurityOrganisation: Turkey," 2018. [Online]. Available: https://ccdcoe.org/library/publications/national-cyber-security-organisation-turkey/.
[56] "SOME (Siber Olaylara Müdahale Ekibi)," BGA Security, 02 November 2018. [Online]. Available: https://www.bgasecurity.com/2018/11/some-siber-olaylara-mudahale-ekibi-nedir/.
[57] "Siber Güvenlik (Cyber Security)," T.C. Ulaştırma ve Altyapı Bakanlığı (The Republic of Turkey - Ministry of Transport and Infrastructure), [Online]. Available: https://www.uab.gov.tr/siber-guvenlik.
[58] "Octopus Cybercrime Community - Turkey," COUNCIL OF EUROPE, 24 November 2017. [Online]. Available: https://www.coe.int/en/web/octopus/country-legislative-profile/-/asset_publisher/LA6eR74aAohY/content/turk-1?inheritRedirect=false&redirect=https%3A%2F%2Fwww.coe.int%2Fen%2Fweb%2Foctopus%2Fcountry-legislative-profile%3Fp_p_id%3D101_INSTANCE_LA6eR74aAohY%26p_p_lifecycle%3D0%26p_p_state%3Dnormal%26p_p_mode%3Dview%26p_p_col_id%3Dcolumn-4%26p_p_col_count%3D2.
[59] "Cyber Security Institute," TÜBİTAK(Türkiye Bilimsel ve Teknolojik Araştırma Kurumu), [Online]. Available: https://sge.bilgem.tubitak.gov.tr/en/kurumsal/cyber-security-institute.
[60] "Cybercrime," Tthe European Union and The Council of Europe, 26 October 2011. [Online]. Available: https://rm.coe.int/16802f6a34.
[61] "KURUMSAL," [Online]. Available: https://www.ssb.gov.tr/WebSite/contentlist.aspx?PageID=19&LangID=1.
[62] "Dosya:Türkiye Cumhuriyeti Ulaştırma, Denizcilik ve Haberleşme Bakanlığı logo.png," 30 January 2019. [Online]. Available: https://tr.wikipedia.org/wiki/Dosya:T%C3%BCrkiye_Cumhuriyeti_Ula%C5%9Ft%C4%B1rma,_Denizcilik_ve_Haberle%C5%9Fme_Bakanl%C4%B1%C4%9F%C4%B1_logo.png.
[63] "Ulusal Siber Olaylara Müdahale Merkezi," 23 May 2019. [Online]. Available: https://tr.wikipedia.org/wiki/Ulusal_Siber_Olaylara_M%C3%BCdahale_Merkezi.
[64] "BİLİŞİM ve BİLGİ GÜVENLİĞİ İLERİ TEKNOLOJİLER ARAŞTIRMA MERKEZİ," [Online]. Available: https://bilgem.tubitak.gov.tr/tr/kurumsal/tanitim-materyalleri.
[65] "Ana Sayfa," [Online]. Available: https://www.egm.gov.tr/.
[66] "Ana Sayfa," [Online]. Available: https://www.tsk.tr/.
[67] "Ana Sayfa," [Online]. Available: http://www.mit.gov.tr/.
[68] "SİBER SUÇLARLA MÜCADELE DAİRE BAŞKANLIĞI," [Online]. Available: https://www.egm.gov.tr/siber.
[69] "Ayyıldız Tim," 30 June 2019. [Online]. Available: https://tr.wikipedia.org/wiki/Ayy%C4%B1ld%C4%B1z_Tim.
[70] "RedHack," 25 February 2019. [Online]. Available: https://tr.wikipedia.org/wiki/RedHack.
[71] "TurkHackTeam," 10 July 2019. [Online]. Available: https://tr.wikipedia.org/wiki/TurkHackTeam.
[72] "Türk Güvenliği," 06 July 2019. [Online]. Available: https://tr.wikipedia.org/wiki/T%C3%BCrk_G%C3%BCvenli%C4%9Fi.
[73] "Three Redhack Suspects Released, One to Testify," Hürriyet Daily News, 26 November 2012. [Online]. Available: http://www.hurriyetdailynews.com/three-redhack-suspects-released-one-to-testify-35479.
[74] "Turkish High School Student Detained for Hacking National School System," Hürriyet Daily News, 18 January 2019. [Online]. Available: http://www.hurriyetdailynews.com/turkish-high-school-student-detained-for-hacking-national-school-system-140611.
[75] "Court Rules to Release on Bail Two Turkish Journalists in Hacking Case," Hürriyet Daily News, 06 December 2017. [Online]. Available: http://www.hurriyetdailynews.com/court-rules-to-release-on-bail-two-turkish-journalists-in-hacking-case-123692.
[76] "Sosyal Medya Davası: Mahir Kanaat ve Tunca Öğreten Hakkında Tahliye Kararı," İstanbul Gerçeği, 06 December 2017. [Online]. Available: https://www.istanbulgercegi.com/sosyal-medya-davasi-mahir-kanaat-ve-tunca-ogreten-hakkinda-tahliyekarari_143561.html.
[77] N. Kurt, "RedHack Davasında Tahliye," Hürriyet, 27 11 2012. [Online]. Available: http://www.hurriyet.com.tr/gundem/redhack-davasinda-tahliye-22015260.
[78] "RedHack Davası: Duygu Kerimoğlu, Alaaddin

Karagenç, Uğur Cihan Okutulmuş Tahliye Oldu.," Başka, 26 November 2012. [Online]. Available: http://www.baskahaber.org/2012/11/redhack-davas-basla-internetim-ve.html.
[79] T. Işık, "2 Bin 824 Öğrenci 'İçeride'," Radikal, 07 August 2012. [Online]. Available: http://www.radikal.com.tr/turkiye/2-bin-824-ogrenci-iceride-1096449/.
[80] "Redhack Operasyonu Patladı! 14 Kişi Serbest!," Muhafelet, 25 November 2013. [Online]. Available: http://muhalefet.org/haber-redhack-operasyonu-patladi-14-kisi-serbest-0-8667.aspx.
[81] "Cyber-Warrior Akıncılar," Wikipedia, 23 January 2019. [Online]. Available: https://fr.wikipedia.org/wiki/Cyber-Warrior_Ak%C4%B1nc%C4%B1lar.
[82] "Judicial System of Turkey," WIKIPEDIA, 11 July 2019. [Online]. Available: https://en.wikipedia.org/wiki/Judicial_system_of_Turkey.
[83] N. Bacanak, "Legal Systems in Turkey: Overview," Thomson Reuters Practical Laws, 01 August 2018. [Online]. Available: https://uk.practicallaw.thomsonreuters.com/w-016-2851?transitionType=Default&contextData=(sc.Default)&firstPage=true&bhcp=1.
[84] İ. Aksel, "Turkish Judicial System," Council of Europe, 2013. [Online]. Available: https://rm.coe.int/turkish-judicial-system-bodies-duties-and-officials-by-ismail-aksel-ju/168078f25f.
[85] "Secularism in Turkey," WIKIPEDIA, 02 August 2019. [Online]. Available: https://en.wikipedia.org/wiki/Secularism_in_Turkey.
[86] "Armenian exchange student arrested in Istanbul on child pornography charges," Hürriyet Daily News, 15 January 2018. [Online]. Available: http://www.hurriyetdailynews.com/armenian-exchange-student-arrested-in-istanbul-on-child-pornography-charges-125761.
[87] "TUNCA-MAHİR İDDİANAME," 2017. [Online]. Available: https://expressioninterrupted.com/tr/wp-content/uploads/2017/10/Tunca-Ogreten-Mahir-Kanaat-Iddianame.pdf.
[88] Z. Hafızoğulları and E. A. Eşitli, "Ceza ve Ceza Usul Hukuku Sitesi," 2010. [Online]. Available: http://www.baskent.edu.tr/~zekih/uygulamaci/.
[89] P. Paganini, "A Turkish Hacker Scores a Record Jail Sentence of 334 Years," Security Affairs, 12 January 2016. [Online]. Available: https://securityaffairs.co/wordpress/43513/cyber-crime/turkish-hacker-334-years-sentence.html.
[90] D. Yaman, "Röntgenci Çalışana Üst Sınırdan HapisÇıktı," Sabah, 21 July 2019. [Online]. Available: https://www.sabah.com.tr/gundem/2019/07/21/rontgenci-calisana-ust-sinirdan-hapis-cik
[91] Ministry of Justice Sweden, "The Swedish Judicial System", Elanders, 2015.
[92] "www.cert.se", *Cert.se*, 2004. [Online]. Available: https://www.cert.se/.
[93] Government Offices of Sweden, "Penal Code", Swedish Government, Stockholm, 2015.
[94] T. Fisher, "What Is The Pirate Bay File Sharing Site? How Do I Use It?", Lifewire, 2019. [Online]. Available: https://www.lifewire.com/pirate-bay-guide-3483018.
[95] "Pirate Bay hit with legal action", News.bbc.co.uk, 2018. [Online]. Available: http://news.bbc.co.uk/2/hi/technology/7219802.stm.
[96] Pirate Bay Verdict Report. Stockholm: STOCKHOLM DISTRICT COURT, 2010. [Online]. Available: https://www.ifpi.org/content/library/Pirate-Bay-verdict-English-translation.pdf
[97] M. Ricknäs, "Pirate Bay Appeals Looks Set to Start in September", PCWorld, 2010. [Online]. Available: https://www.pcworld.com/article/191304/article.html.
[98] L. Larsson, "Åtal mot The Pirate Bay kan dröja", Computer Sweden, 2007. [Online]. Available: https://computersweden.idg.se/2.2683/1.135796/atal-mot-the-pirate-bay-kan-droja.
[99] "Day 3 - The Pirate Bay's 'King Kong' Defense", TorrentFreak, 2009. [Online]. Available: https://torrentfreak.com/g-defense-090218.
[100] "EUR-Lex - 32000L0031 - EN - EUR-Lex", Directive 2000/31/EC of the European Parliament, 2000. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32000L0031.
[101] "Day 4 - Pirate Bay Defense Calls Foul Over Evidence", TorrentFreak, 2009. [Online]. Available: https://torrentfreak.com/day-4-pirate-bay-defense-calls-foul-over-evidence-090219/.
[102] "NJA 2008 s. 946", *Lagen.nu*, 2008. [Online]. Available: https://lagen.nu/dom/nja/2008s946.
[103] "JO dnr 5753-2011", *Lagen.nu*, 2011. [Online]. Available: https://lagen.nu/avg/jo/5753-2011.
[104] The Washington Post. *Suspected North Korean cyber attack on a bank raises fears for S. Korea, allies*. [Online]. Available: https://www.washingtonpost.com/world/national-security/suspected-north-korean-cyber-attack-on-a-bank-raises-fears-for-s-korea-allies/2011/08/07/gIQAvWwIoJ_story.html
[105] Symantec. *Four years of DarkSeoul cyberattacks against south Korea continue on anniversary of Korean war*, [Online]. Available: https://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war
[106] Data Breach Today. *South Korea credit card breach grows*. [Online]. Available: https://www.databreachtoday.com/south-korea-credit-card-breach-grows-a-6437
[107] The Telegraph. *Credit card details of 20m south Koreans leaked* [Online]. Available: https://www.telegraph.co.uk/technology/internet-security/10584348/credit-card-details-of-20m-south-koreans-leaked.html
[108] Kotaku. *Korean overwatch hackers arrested, hit with $10,000 fine*. [Online]. Available: https://kotaku.com/korean-overwatch-hackers-arrested-hit-with-10-000-fin-1825701300
[109] Tech Crunch. *An overwatch hacker in south korea just got sentenced to a year in prison.* [Online]. Available: https://techcrunch.com/2018/06/25/overwatch-hacker-seoul-jail-time/
[110] Thai Visa. *Big Joke arrests South Korean wanted for running child porn website*. [Online]. Available: https://forum.thaivisa.com/topic/1061078-big-joke-arrests-south-korean-wanted-for-running-child-porn-website
[111] Herald Corp. *Four non-partners, 37% suing copyright law*. [Online]. Available: http://news.heraldcorp.com/view.php?ud=20160418000151
[112] Namu Wiki. *Waterpark women's changing room voyeur case* [Online]. Available: http://tiny.cc/pmzebz
[113] Namu Wiki. *Cheongju minor group sexual assault case* [Online]. Available: http://tiny.cc/7ozebz
[114] Cybercrime Law. *Cybercrime laws of South Korea* [Online]. Available: https://www.cybercrimelaw.net/Korea.html
[115] Supreme Court of Korea. *Introduction* [Online]. Available: https://eng.scourt.go.kr/eng/judiciary/introduction.jsp
[116] Wikipedia. *Law enforcement in South Korea*. [Online]. Available: https://en.wikipedia.org/wiki/law_enforcement_in_south_korea
[117] Wikipedia. National Police Agency (South Korea). [Online]. Available: https://en.wikipedia.org/wiki/national_police_agency_(south_korea)
[118] ITU. *Global Cybersecurity Index & Cyberwellness Profiles*. [Online]. Available: https://www.itu.int/dms_pub/itu-d/opb/str/d-str-secu-2015-pdf-e.pdf
[119] Korea Law Translation Center. [Online]. Available: https://elaw.klri.re.kr/eng_service/lawview.do?hseq=28627&lang=eng
[120] OECD. *Criminal Act*. [Online]. Available: https://www.oecd.org/site/adboecdanti-corruptioninitiative/46816472.pdf

[121] Wikipedia. *South Korea Cyber Attacks*. [Online] Available: https://en.wikipedia.org/wiki/2013_south_korea_cyberattack
[122] KrCERT. Big Data. [Online]. Available: https://www.krcert.or.kr/bigdata/introduce.do
[123] RefWorld. *Criminal Code South Korea*. [Online]. Available: https://www.refworld.org/docid/3f49e3ed4.html
[124] National Police Agency Cyber Bureau. *Cybercrime*. [Online]. Available: http://cyberbureau.police.go.kr/eng
[126] Anne Bennett and Michael J. Assels. Computer security at Concordia: Past problems, proposed plans.
[Online], 1995–1998. Available: http://spectrum.library.concordia.ca/980620/.
[127] Lexum. *Judgments of the Supreme Court of Canada*. [Online]. Available: https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/17515/index.do
[128] Local 21 News. *Lower Allen man facing charges for illegally recording people in their home.* [Online]. Available: https://local21news.com/news/local/lower-allen-man-facing-charges-for-illegal-recording-people-in-their-homes
[129] Supreme Court of Canada. *Cole Appellants Factum*. [Online]. Available: http://aspercentre.ca/wp-content/uploads/2017/06/R-v-Cole-Appellants-Factum.pdf
[130] Office of Privacy Commissioner of Canada. *Canadian adware developer Wajam Internet Technologies Inc. breaches multiple provisions of PIPEDA*. [Online]. Available: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2017/pipeda-2017-002/
[131] CBC. *She secretly recorded her husband's alleged plot to kill her. A judge threw out the tape. Here's why*. [Online]. Available: https://www.cbc.ca/news/canada/saskatoon/nicholson-vey-murder-trial-secret-recording-1.5153175
[132] J. Bronskill, "Canada Among Targets of Alleged Chinese Hacking Campaign," CBC, 20 December 2018. [Online]. Available: https://www.cbc.ca/news/politics/canada-among-china-hacking-victims-1.4954608.
[133] S. O`Shea, "Lawsuits Hit Canadians Accused of Illegal Downloading, Uploading of Movies," Global News, 6 February 2019. [Online]. Available: https://globalnews.ca/news/4933339/lawsuits-movie-downloading-uploading/.
[134] E. Raymer, "No Expectation of Privacy in Child-luring Cases on the Internet, SCC Rules," Canadian Lawyer, 18 April 2019. [Online]. Available: https://www.canadianlawyermag.com/practice-areas/criminal/no-expectation-of-privacy-in-child-luring-cases-on-the-internet-scc-rules/276059
[135] Security Boulevard. *Capital One Data Breach: A reminder to lock your back door*. [Online]. Available: https://securityboulevard.com/2019/08/capital-one-data-breach-a-reminder-to-lock-your-back-door/
[136] Royal Canadian Mounted Police. *Defiant Tech Inc. Enters Guilty Plea Following RCMP Cybercrime Investigation*. [Online]. Available: http://www.rcmp-grc.gc.ca/en/news/2019/defiant-tech-inc-enters-guilty-plea-rcmp-cybercrime-investigation
[137] CBC. *4 executives of Vancouver's PacNet Services charged in international mail fraud scheme*. [Online].
Available: https://www.cbc.ca/news/canada/british-columbia/bc-pacnet-executives-charged-mail-fraud-1.5183671
[138] iPolitics. *Canada to ratify Budapest Convention on Cybercrime*. [Online].
Available: https://ipolitics.ca/2015/05/05/canada-to-ratify-budapest-convention-on-cybercrime/
[139] P. Bermúdez. *Políticas y Estrategias del Gobierno Nacional en materia de Seguridad de la Información y Ciberseguridad.* [Online].
Available:
http://portal.uasb.edu.ec/UserFiles/385/File/CBA_Patricio%20Bermudez.pdf
[140] "Agreement on Government Procurements, "WIKIPEDIA,01 July 2019. [Online].
Available:
https://en.wikipedia.org/wiki/Agreement_on_Government_Procurement
[141] "Global Cloud Computing Scoreboard," The SoftwareAlliance,2012. [Online].
Available: https://cloudscorecard.bsa.org/2012/assets/PDFs/country reports/Country_Report_Turkey_en.pdf

[142] L. Moran, "Swedish schoolkids hack computers to change grades, fend off alerts to parents", *Nydailynews.com*, 2014. [Online].
Available: https://www.nydailynews.com/news/world/swedish-schoolkids-hack-computers-change-grades-article-1.1753362.
[143] "Ruling Swedish party's Twitter account hacked", *BBC News*, 2019. [Online].
Available: https://www.bbc.com/news/world-europe-47935251.
[144] C. Cimpanu, "DDoS Attacks Cause Train Delays Across Sweden", *BleepingComputer*, 2017. [Online].
Available: https://www.bleepingcomputer.com/news/security/ddos-attacks-cause-train-delays-across-sweden/.
[145] "Hot Line Riot from 1982", *Fffff.at*, 2007. [Online].
Available: http://fffff.at/hot-line-riot-from-1982/.
[146] "Spanish doctor charged with child sex abuse in Sweden", *Thelocal.com*, 2018. [Online].
Available: https://www.thelocal.com/20180912/spanish-doctor-charged-with-child-sex-abuse-in-sweden.
[147] European Central Bank, "Fifth report on card fraud", European Central Bank, Frankfurt, 2018.
[148] A. Alexandre, "Swedish Crypto Exchange QuickBit Announces User Data Breach", *Cointelegraph*, 2019. [Online]. Available: https://cointelegraph.com/news/swedish-crypto-exchange-quickbit-announces-user-data-breach.
[149] M. Gromek, "New Cryptocurrency Wave Of Fraud Hits Instagram In Sweden", *Forbes.com*, 2019. [Online].
Available: https://www.forbes.com/sites/michalgromek/2019/03/11/new-cryptocurrency-wave-of-fraud-hits-instagram-in-sweden/#6c7f921a7a39
.[150] A. Hellström and E. Myrberg, "Sweden Cybersecurity 2019", *ICLG*, 2018. [Online].
Available: https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/sweden.
[151] European Union, "EUGDPR", European Union, 2016.