# NEW TRENDS IN CRIMINAL LAW - RISE OF CYBERCRIME

Gjorgi Slamkov, page 123-140


## ABSTRACT

Crime is a dynamic and evolutionary phenomenon that uses the scientific and technological achievements to achieve the set goals. A criminal-legal reaction, especially the criminal law as a substantive part, ie., a set of norms that define socially harmful behavior with a threat of sanction, is also in constant evolution, in order to meet the challenges of today.

Modern society is facing various forms of criminal activities. It is possible that the categorization is done according to various criteria, but what is specifically the subject of interest are the forms of punishable behavior that are a hallmark of the achieved level of civilization development, the behaviors that have a universal detrimental effect, and, of course, what steps are taken in the criminal law in response to new challenges.

In the paper focus is on the cybercrime as one of the most recent forms of punishable behavior, but with enormous growth, harmful consequences expressed in billions, great mystery, and serious difficulties in providing evidence.

The paper puts emphasis on cybercrimes that more often occur in practice, international regulations, as well as national strategies of some countries.


**Key words:** cybercrime, internet, criminal law, criminal offenses,

**Gjorgi Slamkov, PhD**

**e-mail: gj.slamkov@yahoo.com**

**Article type:**

**UDK:** 343.9:004.7

**Date of received:**
**August 19, 2018**

**Date of acceptance:**
**September 19, 2019**

**Declaration of interest:**
The author reported no conflict of interest related to this article.

## Inroduction

The one of the fastest-growing areas of technical infrastructure development is Internet. Today, information and communication technologies are omnipresent and the trend towards digitization is growing. The demand for Internet and computer connectivity has led to the integration of computer technology into products that have usually functioned without it. Electricity supply, transportation infrastructure, military services and logistics – virtually all modern services depend on the use of information and communication technologies.

The influence of new technologies on society goes far beyond establishing basic information infrastructure. The availability of new technologies is a foundation for development in the creation, availability and use of network-based services. So, e-mails have displaced traditional letters, online web representation is nowadays more important for businesses than printed publicity materials.

However, the growth of the information society is accompanied by new and serious threats. Attacks against information infrastructure and Internet services now have the potential to harm society in new and critical ways. As a result of the massive use of cyberspace to carry out everyday activities, then, doing business operations, etc., the space of action of cybercriminals increases. Namely, in 2015 cybercrime costs the world $ 3 trillion. It is estimated that in 2021 the amount of damage will be $ 6 trillion (https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf).

The fight against cybercrime requires a serious approach, for this purpose several countries have drafted strategic documents. Generally, in them, the focus is placed on several strategic goals, such as: legal measures, technical and procedural measures, organizational structures, capacity building and international cooperation.

The technical measures alone cannot prevent any crime, it is critical that law-enforcement agencies are allowed to investigate and prosecute cybercrime effectively.

Cybercrime has an international character and therefore raises the need for state cooperation in efforts to prevent it. On the normative field, one of the most important legal documents to combat cybercrime is the Council of Europe's Convention on Cybercrime.

## 1. Rise of cybercrime

Although there is no single universal definition of cybercrime, however, two basic types of internet-related criminal offenses can be found in theory (https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime):

- High-level computer crime - sophisticated attacks on computer hardware and software and

- Criminal offenses provided through the Internet - traditional offenses that take a different form when committed online, for example crimes against finances, then acts against children, etc.

Generally speaking, cyber crimes are any crimes that involve a computer and a network. In some cases, the computer may have been used in order to commit the crime, and in other cases, the computer may have been the target of the crime.

The question arises of the difference between cybercrime and traditional criminal activity. It is a fact that the digital computer alone can not commit crimes, but it is also known that even before the prefix "cyber" criminals committed crimes such as fraud, privacy violation, identity theft. In this sense, cybercrime, especially online involvement, is a continuation of existing criminal behavior along with some new illegal activities, but in a sophisticated way with high speed in the the commission of the crime and much more difficulty in documenting and proving it.

Basically, cybercrime is an attack on information for individuals, corporations or governments. Although attacks do not occur on a physical body, they take place on the personal or corporate virtual body, which is a set of informational attributes that define people and institutions on the Internet. In other words, in the digital age, our virtual identities are essential elements of everyday life: we are a package of numbers and identifiers in multiple computer databases owned by governments and corporations.

Cybercrime has a universal character, it is impossible to present in a local or national character. The global network that creates a world without borders and allowing people to gain benefits that were previously difficult to access at the same time be abused by criminals to cause harmful consequence for an entity. Perhaps there are more difficulties in providing evidence for crimes committed through cybercrime, but traces remain for these crimes and for effective and efficient fight against them requires appropriate international cooperation, that is, often they are crimes of supranational character.

### 1.1. *Crimes in the area of cybercrime*

Cybercrime covers a range of punishable behaviors, namely, on one side there are crimes involving fundamental privacy violations, such as attacks on the integrity of information stored in digital deposits and the use of illegally obtained digital information on blackmail of a firm or individual. Also, this includes crime of identity theft. Next are crimes based on transactions, such as fraud, trafficking in child pornography, money laundering and counterfeiting. Another part of this type of crime involves individuals within corporate or government bureaucracies who deliberately change data on profits or political goals. On the other hand are those crimes involving attempts to disrupt the actual operation of the Internet. These range from spamming, hacking, denial of service, attacks on certain sites, to cyberterrorism.

**Cybercrime most often occurs in the following types:**

a) **Hacking**

Hacking in simple terms means an illegal intrusion into a computer system and/or network. A hacker is someone who seeks to breach defenses and exploit weaknesses in a computer system or network. The offence described as –hacking, refers to unlawful access to a computer system, one of oldest computer-related crimes. Following the development of computer networks, this crime has become a mass phenomenon. Famous targets of hacking attacks include the US National Aeronautics and Space Administration (NASA), the US Air Force, the Pentagon, Yahoo, Google, eBay, the German Government. (www.hackerwatch.org). Hackers may be motivated by a multitude of reasons, such as profit, protest, information gathering, challenge, recreation.

b) **Denial of service attacks**

In computing, a denial-of-service attack (DoS attack) is a cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. DoS attacks target specific computer systems. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled. A DoS attack makes computer resources unavailable to their intended users. By targeting a computer system with more requests than the computer system can handle, offenders can prevent users from accessing the computer system, checking e-mails, reading the news, booking a flight or downloading files.

### c) Virus dissminition

A computer virus is a type of malicious software program ("malware") that, when executed, replicates itself by modifying other computer programs and inserting its own code. Computer viruses currently cause billions of dollars' worth of economic damage each year, due to causing system failure, wasting computer resources, corrupting data, increasing maintenance costs, etc. The term "virus" is also commonly used to refer to other types of malware. "Malware" encompasses computer viruses along with many other forms of malicious software, such as computer "worms", ransomware, spyware, adware, trojan horses, keyloggers, rootkits, and other malicious software.

### d) Cyber terrorism

Cyberterrorism means that terrorists could cause massive loss of life, worldwide economic chaos and environmental damage by hacking into critical infrastructure systems (https://link.springer.com/chapter/10.1007/978-1-4939-0962-9_1). The nature of cyberterrorism is conducts involving computer or Internet technology that: is motivated by a political, religious or ideological cause; is intended to intimidate a government or a section of the public to varying degrees, or seriously interferes with infrastructure.

NATO defines cyberterrorism as "a cyberattack using or exploiting computer or communication networks to cause sufficient destruction or disruption to generate fear or to intimidate a society into an ideological goal" (http://searchsecurity.techtarget.com/definition/cyberterrorism). The FBI defines it as, "premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by subnational groups or clandestine agents" (https://leb.fbi.gov/articles/featured-articles/cyber-terror).

### e) Software piracy

That is theft of software through the illegal copying of genuine programs or the counterfeiting and distribution of products intended to pass for the original. Software piracy is the stealing of legally protected software. Under copyright law, software piracy occurs when copyright protected software is copied, distributed, modified or sold. Software piracy is considered direct copyright infringement when it denies copyright holders due compensation for use of their creative works.

The majority of software today is purchased as a one-site license, meaning that only one computer may have that software installed on it at one time. Copying that software to multiple computers or sharing it with your friend without multiple licenses is considered software piracy, which is illegal.

It is a phenomenon on a large scale, namely, over half of the world's computer users- 57%- admit they pirate software. The steadily developing world drove the commercial value of software theft to $63.4 billion (https://sites.google.com/site/softwarepiracywiki12/software-piracy ).

### f) Tax-refund fraud

Fraud for collecting a tax on identity theft occurs when someone uses someone else's identifying information, such as name, social security number or other identification information, without permission, in order to commit fraud or other crimes. The scam usually occurs when "an identity thief uses a legitimate taxpayer's identity to file a fraudulent tax return and claim a refund. Generally, the identity thief will use a stolen SSN to file a forged tax return and attempt to get a fraudulent refund early in the filing season". By filing the fraudulent tax return early, of course, the identity thief usually receives the refund before the victim sends his or her tax return, and the IRS processes it.

An essential requirement for committing this crime is the theft of information about the person filing a tax return. The most sensitive point are the databases of taxpayers, namely, through the unauthorized entry into them a huge material is collected and it is the basis for the fraud. In any case, here we have the subsequent execution of several cybercrimes.

This crime is particularly prevalent in the United States, namely, for the tax return processing year of 2011 (after tax year 2010 tax returns), the IRS reported 938,664 cases of identity theft fraud theft fraud, with about 6.5 billion in fraud tax returns issued. (http://www.fraud-magazine.com/article.aspx?id=4294982014).

### g) Identity theft

Identity theft, also known as identity fraud, is a crime in which an imposter obtains key pieces of personally identifiable information in order to impersonate someone else.

Identity theft is categorized two ways: true name and account takeover. True-name identity theft means the thief uses personal information to open new accounts. Account-takeover identity theft means the imposter uses personal information to gain access to the person's existing accounts. Typically, the thief will change the mailing address on an account and run up a huge bill before the person whose identity has been stolen realizes there is a problem. The internet has made it easier for an identity thief to use the information they've stolen, because transactions can be made without any personal interaction.

The type of data the perpetrators target varies, the most relevant data are social security and passport numbers, date of birth, address and phone numbers, and passwords. Social security number used, for example, in the United States is a classic example of a single identity-related data item that perpetrators target. The perpetrators can use the social security number and passport information to open financial accounts, to take over existing financial accounts, to obtain credit.

Date of birth, address and phone numbers can, in general, be used to commit identity theft if they are combined with other pieces of information. Having access to additional information like date of birth and address can help the perpetrator to circumvent verification processes. One of the greatest dangers related to that information is the fact that it is currently available on a large scale on the Internet – either published voluntarily in one of the various identity-related for or based on legal requirements as imprint on websites.

The damage from identity theft is expressed in millions of dollars. But they also cause damage to the reputation of the victim. That is why some Identity theft is not reported, which means that damage from them is much higher, ie it has a "dark number".

### h) **Theft of sensitive data**

Data theft is the act of stealing digital information stored on computers, servers, or electronic devices of an unknown victim with the intent to compromise privacy or obtain confidential information. Information can include anything from financial information, like credit card numbers or bank accounts, to personal information, like social security numbers, drivers license numbers, and health records. Once only the problem of large businesses and organizations, data theft is a growing problem for everyday computer users (http://safety.lovetoknow.com/personal-safety-protection/what-is-data-theft).

i) **Computer-related forgery**

Computer-related forgery describes the manipulation of digital documents. The offence can, for example, be committed by creating a document that appears to originate from a reliable institution, manipulating electronic images or altering text documents.

Often, offenders send out e-mails that look like communications from legitimate financial institutions used by the target. The e-mails are designed in a way that it is difficult for targets to identify them as fake e-mails. The e-mail asks recipient to disclose and/or verify certain sensitive information. Many victims follow the advice and disclose information enabling offenders to make online transfers etc.

In the past, prosecutions involving computer-related forgery were rare, because most legal documents were tangible documents. Digital documents play an ever more important role and are used more often. The substitution of classic documents by digital documents is supported by legal means for their use, e.g. by legislation recognizing digital signatures. Criminals have always tried to manipulate documents. With digital forgeries, digital documents can now be copied without loss of quality and are easily manipulated.

## 1.2. *Harmful consequences of cybercrime*

In today's world, it's difficult to get through the day without interaction of a cell phone, computer, or other electronic devices connected to the internet. Technology, today, is simply all around us in everything we do, from work to our leisure time. We use technology to perform our jobs every day, leaving us vulnerable to cyber attacks whenever we get online. Cyber criminals have become the world's most dangerous criminals simply because they can act covertly and from anywhere in the world.

One of the main consequences of cybercrime on a company is a loss of revenue/income. This loss may be caused by an outside person who acquires sensitive financial information, using it to extract funds from an organization. It can also come about when a business's e-commerce site becomes compromised--while terminal, expensive income is lost when consumers are unable to utilize the site. Another major consequence of cybercrime is the time that is wasted when Information Technology personnel must dedicate maximum part of their day handling such incidences. Rather than working on productive and creative measures for an organization, many Information Technology staff members spend a great percentage of their time handling security breaches and other problems related with cybercrime.

In situations where customer records are compromised by a security contravene associated with cybercrime, a company's reputation can take a major batter. Customers whose credit cards or other monetary data become grabbed by hackers or other infiltrators drop assurance in an organization and often begin taking their business elsewhere. Besides that, due to the safety measures that many companies must implement to neutralize cybercrime, there is often a pessimistic effect on employees' efficiency, it means reducing productivity.

Currently, companies in the United States experience an annual loss of more than hundreds of millions US dollars due to cybercrime with the majority of these losses stemming from malicious code and denial of service attacks. The statistic shows the amount of damages caused by cybercrime reported to the Internet Crime Complaint Centar - IC3 (https://www.ic3.gov/default.aspx) from 2001 to 2016. In the 2016, the annual loss of complaints referred to the IC3 amounted to 1.33 billion U.S. dollars, up from 781.84 million U.S. dollars in 2013. The most costly cyber attack consequences for global companies in 2016 were losses suffered through business disruption and information loss. That year, the majority of data breach incidents were related to identity theft, followed by financial and account access (https://www.statista.com/statistics/267132/total-damage-caused-by-by-cyber-crime-in-the-us/).

Data breaches and their consequences have also had profound effects on consumers with personal information and credit details being stolen. The biggest online data breach compromised more than 3 billion user accounts (https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html). Online brands with the highest chance of being targeted by phishing attacks include online payment provider Paypal and online auction house eBay, as well as numerous online service providers that require personal identification as well as payment information (https://www.statista.com/statistics/290525/cyber-crime-biggest-online-data-breaches-worldwide).

There are predictions that by 2021, cybercrime losses are expected to cost the world $ 6 trillion (https://www.csoonline.com). While there are numerous contributors to the rise in cybercrime -- which is expected to cost the world more than $6 trillion by 2021, up from $3 trillion in 2015 -- the most obvious predictor is a massive expansion of the global attack surface which hackers target. The cybercrime cost prediction includes damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm. Cyber threats have evolved from targeting and harming computers, networks, and smartphones — to humans, cars, railways, planes, power grids and anything with a heartbeat or an electronic pulse. As the planet morphs into a digital global society of interconnected people, places, and things, there's a whole cyberspace that needs to be defended.

## 2. Cybersecurity Strategies

Taking into account the serious negative consequences that result from cybercrime, many countries have adopted strategies to deal with this socially harmful behavior. They include the strategic goals that are generally repeated, however, certain countries place the emphasis on the national segment, while others set goals of a global character, so:

- Australia – Cyber Security Strategy, 2009 (https://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf),

the objectives of the australian government's cyber security policy are:

1. All Australians are aware of cyber risks, secure their computers and take steps to protect their identities, privacy and finances online.
2. Australian businesses operate secure and resilient information and communications technologies to protect the integrity of their own operations and the identity and privacy of their customers
3. The Australian Government ensures its information and communications technologies are secure and resilient.

- Canada - Canada's Cyber security Strategy, 2010 (https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf),

Canada's Cyber Security Strategy is built on three pillars:

1. Securing Government systems;
2. Partnering to secure vital cyber systems outside the federal Government;
3. Helping Canadians to be secure online.

- France – Défense et securité des systems d'information – Stratégie de la France, 2011

  (https://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf),

  1. To be a global cyber defense power;
  2. Guarantee France's freedom of decision by protecting the information of sovereignty;
  3. Strengthen cybersecurity of national vital infrastructures;
  4. Ensuring security in cyberspace.

- Germany –Cyber Security Strategy for Germany, 2011 (https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile),

The Federal Government has specifically focus on this strategic areas:

1. Protection of critical information infrastructures;
2. Secure IT systems in Germany;
3. Strengthening IT security in the public administration;
4. Effective crime control also in cyberspace;
5. Effective coordinated action to ensure cyber security in Europe and worldwide.

- United Kingdom - The UK Cyber Security Strategy, 2011 (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf),

the objectives of the UK cyber security policy are:

1. The UK to tackle cybercrime and be one of the most secure places in the world to do business in cyberspace;

2. The UK to be more resilient to cyber attacks and better able to protect our interests in cyberspace;

3. The UK to have helped shape an open, stable and vibrant cyberspace which the UK public can use safely and that supports open societies;

4. The UK to have the cross-cutting knowledge, skills and capability it needs to underpin all our cyber security objectives.

- USA – Cyber Strategy,2015

(https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf).

Ministry of Defense or DoD sets five strategic goals for its cyberspace missions:

1. Build and maintain ready forces and capabilities to conduct cyberspace operations;

2. Defend the DoD information network, secure DoD data, and mitigate risks to DoD missions;

3. Be prepared to defend the U.S. homeland and U.S. vital interests from disruptive or destructive cyberattacks of significant consequence;

4. Build and maintain viable cyber options and plan to use those options to control conflict escalation and to shape the conflict environment at all stages;

5. Build and maintain robust international alliances and partnerships to deter shared threats and increase international security and stability.

Cybersecurity strategies are setting policy goals, measures and

institutional responsibilities in a fairly succinct manner. Generally, the primary concern is to ensure the confidentiality, integrity and availability of computer data and systems and to protect against or prevent intentional and non-intentional incidents and attacks. The approach to cybercrime in a specific country is influenced by many factors, including the nature of the threat, the state of the criminal justice system, the level of respect for human rights and the rule of law.

The Strategies provided measures to combat cybercrime in several directions, such as:

a) *Cybercrime reporting and intelligence* - gathering information or cybercrime intelligence is an essential step in fighting it, as this creates conditions for preventing cybercrime or reducing harmful consequences.

b) *Prevention* - preventive measures are defense mechanisms that prevent the creation of conditions for the commission of cybercrime. Through their active implementation the possibility of cybercrime has been reduced.

c) *Legislation* - normative solutions in which will be incorporated international standards for determining the criminal offense, for conducting the criminal procedure, as well as standards for protection of human rights. That is, they are the basic solutions for the efficiency of the procedure and for the protection of human rights.

d) *Strengthening the institutional capacities* - the fight against cybercrime requires specially educated and trained staff. In addition, the training should cover how the problems that have been revealed so far in practice, and those that would arise in the future, that is, ie. to be in step with cybercriminals.

e) *International cooperation* - cybercrime is transnational crime involving multiple jurisdictions. Efficient international police and judicial cooperation is required to preserve volatile electronic evidence. This includes direct cooperation between high-tech crime units and between prosecutors of different countries.

## 3. International legal documents on the fight against cybercrimes

### *3.1. Council of Europe Convention on Cybercrime*

The Convention on Cybercrime, also known as the Budapest Convention on Cybercrime (www.coe.int/cybercrime), is the first international treaty seeking to address Internet and computer crime by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations. It was drawn up by the Council of Europe in Strasbourg, France, with the active participation of the Council of Europe's observer states Canada, Japan, Philippines, South Africa and the United States.

The Convention and its Explanatory Report was adopted by the Committee of Ministers of the Council of Europe in November 2001. It was opened for signature in Budapest, on 23 November 2001 and it entered into force on 1 July 2004. As of April 2018, 57 states have ratified the Convention. On 1 March 2006, the Additional Protocol to the Convention on Cybercrime came into force. Those States that have ratified the additional protocol are required to criminalize the dissemination of racist and xenophobic material through computer systems, as well as threats and insults motivated by racism or xenophobia.

The Convention structurally covers three parts: substantive criminal law, procedural criminal law, and international criminal assistance.

The Convention aims principally at:

- Harmonising the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime,
- Providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form,
- Setting up a fast and effective regime of international cooperation.

In the first part of the Convention are given more norms that define cybercrimes. The Convention defines the following offences: illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography, and offences related to copyright. These are norms that indicate to the states what behavior should be sanctioned. In addition, here are the norms for responsibility of a legal entity, ancillary liability and sanctions.

Convention sets out such procedural law issues as expedited preservation of stored data, expedited preservation and partial disclosure of traffic data, production order, search and seizure of computer data, real-time collection of traffic data, and interception of content data. Regarding jurisdiction, the following principles are provided: territorial principle, flag principle, principle of registration and universal principle.

The special attention is placed on international cooperation and

assistance in the criminal field, including extradition. The Convention contains a provision of transborder access to stored computer data which does not require mutual assistance and provides for the setting up of a 24/7 network for ensuring speedy assistance among the states (http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf).

### *3.2. United Nations Convention against Transnational Organized Crime*

The main international instrument for judicial cooperation in criminal matters is the United Nations Convention against Transnational Organized Crime (UNTOC) adopted by the United Nations General Assembly on November 15, 2000, and is appointed to serve as the most significant mechanism for fighting Transnational Organized Crime (https://en.wikipedia.org/wiki/United_Nations_Convention_against_Transnational_Organized_Crime).

This convention contains important instruments for international cooperation, but was not specifically designed to address cybercrime-related issues. Nor does it provide specific provisions dealing with urgent requests to preserve data.

The convention is only applicable in cybercrime cases if the offence involves an organized crime group. According to UNTOC organized crime group is a structured group of three or more people.

But the structure of the cybercrime groups is not necessarily comparable to that of traditional organized crime groups. Cybercrime groups tend to have a looser and more flexible structure. In addition, groups are often much smaller compared to traditional organized crime groups. The Internet enables close cooperation with others and coordination of activities without ever having met face-to-face. This makes it feasible for offenders to work together in fluid ad hoc groups.

However, in the part of international cooperation, there are several general norms that create space for cooperation between states in the fight against cybercrime. But these norms do not have the same application for different cybercrimes, starting from the essence of the crime and the manner of execution.

**Conclusion**

In less than two decades, the Internet has grown from a curiosity to an essential element of modern life for millions. The Internet has transformed the way people live and do business. It also bridges the communication divide between people in a cost-effective way. With the erosion of national borders brought about by the Internet, making new friends with people from other countries is much easier.

As with other aspects of globalization, its rapid expansion has far exceeded regulatory capacity, and this absence of authority has left space for many abuses.

Cybercrime has been used to describe a wide range of offences, including offences against computer data and systems, computer-related forgery and fraud, content offences, and copyright offences.

Cybercrime denotes abuse of science and technology achievements. Appears in different types that have financial consequences as well as a privacy breach. Cybercrime is characterized by creating an enormous number of victims, damages in billions of dollars/euros, offenses performed at vast distances, with great difficulty in documenting them.

Criminals, like everyone else with access, make use of the Internet for communication and information gathering, and this has facilitated a number of traditional organized crime activities. But the growing importance of the Internet and our collective dependence on it has also created a number of new criminal opportunities.

International cooperation in the fight against cybercrime is necessary, as the state borders do not interfere with the performance of these offenses. The cooperation involves the adoption of supranational legislation, determination of the offenses, prescribing the procedure, creation of special bodies / agencies for combating cybercrime, as well as the adequate financial support.

**Bibliography:**

1. https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

2. https://link.springer.com/chapter/10.1007/978-1-4939-0962-9_1

3. https://leb.fbi.gov/articles/featured-articles/cyber-terror

4.https://sites.google.com/site/softwarepiracywiki12/software-piracy

5. http://www.fraud-magazine.com/article.aspx?id=4294982014

6. http://safety.lovetoknow.com/personal-safety-protection/what-is-data-theft

7. https://www.ic3.gov/default.aspx

https://www.statista.com/statistics/267132/total-damage-caused-by-by-cyber-crime-in-the-us/

8. https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html

9. https://www.statista.com/statistics/290525/cyber-crime-biggest-online-data-breaches-worldwide

10. https://www.csoonline.com

11. https://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf

12.https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf

13.https://www.ssi.gouv.fr/uploads/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf

14.https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile

15.https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

16.https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

17.www.coe.int/cybercrime

18.http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf

19.https://en.wikipedia.org/wiki/United_Nations_Convention_against_Transnational_Organized_Crime