CYBERTERRORISM: THE LATEST CRIME AGAINST INTERNATIONAL PUBLIC ORDER

Sandra Sophie-Elise OLĂNESCU[*]
Alexandru Vladimir OLĂNESCU[**]

Abstract

Cyberterrorism has become the latest global threat that highlights security leaks in the digital world and its outcomes.

Nowadays economic and social context as well as the advances in the field of information technology facilitated individuals, private entities and governments to become increasingly interconnected through computer structures.

Cyber-attacks have seen an alarming development, and they have been successfully used in paralyzing activities, such as rail, naval and air traffic, being even used by some state entities in military and economic espionage.

Moreover, cyber-attacks have been able to block activities of state institutions, corporations, financial and banking institutions, cross-border trading companies, as well as individuals, viewed as single end users of products or services.

Thus, it would be an understatement to say that cyber terrorism has become a worldwide menace; it is a live global phenomenon that spreads fear whilst being impressively effective in terms of seriousness and widespread damages.

Given the significance of this global negative phenomenon with potential devastating effects, depending on the severity with which it manifests, cyberterrorism has been chosen as the subject matter of this paper.

The aim of the paper is to go into the depth of this global phenomenon, starting from the economic, political, social and technological factors that favored the emergence and hasty development of cyber-terrorism.

Keywords: *cyberterrorism, cybercrime, international public order, Internet, victim*

1. Introduction

In the current social and economic background and taking into account the progress in the field of information technology, individuals and private and governmental entities, in the course of their current activities, are increasingly interconnected by means of IT structures.

There were many cases when cyberattacks have been able to block the activities of state institutions, corporations, financial and banking institutions, cross-border trading companies, by taking on different proportions on individuals, considered as *ut singuli* in the capacity of final users of certain products or service.

Furthermore, in 2017, cyberattacks increased alarmingly, being successfully used in activities carried out in order to block transportation means, respectively rail, naval and air traffic, being used by certain state entities in military and economic espionage.

It should be noted that, given their damaging effects, cyberattacks have begun to be preferred even by terrorist organizations in place of classical assaults, with an even greater impact on society, being able to affect a wider range of individuals (natural persons/legal entities) by means of the immediate effect of these types of criminal activities.

Therefore, the protection of the information systems integrity has become, both for the states and for the individuals, a real concern, *on the one hand*, by the need to provide networks for effective protection of information systems, and, *on the other hand*, at legislative level, by creating a regulatory framework that includes the widest range of illicit activities in order to prevent and protect information systems from "*cybercrime*" activities.

2. Cybercrime and cyberterrorism

In order to be classified as cyberterrorism, virtual space activity must have a '***terrorist'*** component, which means that it must include terror and have a political motivation. Therefore, we have to make the distinction between terrorism that uses information technology as weapon or target and terrorism that simply exploits information technology, this side being the most visible and intensely used at the time being.

At this level, a distinction should be made between *cybercrime* and *cyberterrorism,* the essential tiebreak criterion being represented by the "*terrorist component".*

The notion of "cybercrime" defines all the deeds committed in the area of information technologies, within a certain time period and on a certain criterion. As any social phenomenon, cybercrime represents a system with own properties and functions, distinct from those of the constituent elements in terms of quality.

Although at the international level there is no unanimously accepted legal definition on cyberterrorism, a number of definitions have been formulated at the conventional level, among which we will mention that of the US Federal Bureau of

[*] PhD Candidate, Faculty of Law, Nicolae Titulescu University of Bucharest (e-mail: sandra.olanescu@cliza.ro)

[**] PhD Candidate, Faculty of Law, "Nicolae Titulescu" University of Bucharest (e-mail: alexandru.olanescu@cliza.ro)

Investigation, which is the most eloquent: cyberterrorism is a phenomenon that is "*a premeditated, politically motivated attack against information, computer systems, programs and data which results in violence against noncombatant targets by subnational groups or clandestine agents*"[1].

Cybercrime is one of the fastest-evolving branches of the criminal spectrum, given its specificity, namely:

- the speed that perpetrators can exploit in committing cybercrime through internet;
- the comfort these perpetrators can enjoy at the shelter of anonymity in committing a wide range of illicit activities that do not know physical or virtual boundaries;
- the magnitude of the consequences of these unlawful actions and
- the potential benefits that can be gained from the commission of such crimes.

As far as the European Space is concerned, an important step in identifying, qualifying and attaining criminal responsibility for cyberattacks was made by the adoption of the Directive on attacks against information systems ("*Directive 2013/40/EU*") in 2013, establishing minimal rules on the definition of criminal offences and penalties in the field of the attacks against information systems and providing operational measures to improve cooperation between authorities.

Although Directive 2013/40/EU has led to significant progress in terms of the criminalization of cyberattacks at a comparable level in all Member States, the improvement of the way it is implemented by the national transposition regulations is possible by updating them with the continuous evolution of the cybercrime, this process being certainly achievable with the assistance of the European Commission (the "*Commission*").

Directive 2013/40/EU of the European Parliament and of the Council of August 12th, 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA of the Council, published in the Official Journal of the European Union L 218/8 of August 14th, 2013.

Furthermore, as of 2018, the Commission has been adopting concrete proposals to facilitate rapid cross-border access to electronic evidence, nowadays practical measures being taken to improve cross-border access to electronic evidence for criminal investigations, including the financing for training on cross-border cooperation, the development of an electronic platform for the exchange of information within the European Union and the standardization of forms of judicial cooperation between Member States (*Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*[2].

At the international level, according to INTERPOL, cybercrime can be classified into two major categories of cybercrimes, namely:

- *Advanced cybercrime* (or high-tech crime) – sophisticated attacks against computer hardware and software;
- *Cyber-enabled crimes* – many "*traditional*" crimes have taken a new turn with the advent of the Internet, such as crimes against children, financial crimes, theft, fraud, illegal games, sale of counterfeit medicines and even terrorism.

According to the INTERPOL data, cybercrimes have seen an impressive evolution, their authors changing their profile with the evolution of the crimes: from individuals or small groups, cybercrimes are nowadays committed by complex cybercriminal networks bringing together individuals from across the globe in real time to commit crimes on an unprecedented scale. Such organized criminal groups use increasingly the internet as a means to facilitate their activities and to maximize profit in the shortest time possible[3].

Most importantly, cybercrime is characterized by internationality and a rapid evolution, both at the organizational level in what concerns the perpetrators and at the level of crimes complexity, leading to worsening the consequences resulting from the commission of such crimes, therefore, the security of IT networks and systems appears to be a necessity for any of the "*potential victims*".

3. Relevant international documents on cyberterrorism

Foremost, the Resolution 2133 (2014) adopted by the United Nations Security Council within its 7101st meeting of January 27th, 2014 is one of the most important text to have ever been drafted on cyberterrorism. This document refers to the general phenomenon of terrorism, including the manifestation of cyberterrorism, as follows: "*reaffirming that terrorism in all forms and manifestations constitutes one of the most serious threats to international peace and security and that any acts of terrorism are criminal and unjustifiable regardless of their motivations, whenever and by whomsoever committed and further reaffirming the need to combat by all means, in accordance with the Charter of the United Nations, threats to international peace and security caused by terrorist acts*". It also reveals, among other things, that: it "*reaffirms its resolution 1373 (2001) and in particular its decisions that all States shall prevent and suppress the financing of terrorist acts and refrain from providing any form of support, active or passive, to entities or persons involved in terrorist acts, including by suppressing recruitment of member of terrorist*

[1] White, Kenneth C., *Cyber-terrorism:Modern mayhem*, U.S.Army War College, 13 March 2015;

[2] Available here: http://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52017JC0450&from=EN);

[3] Please see: https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime;

groups and eliminating the supply of weapons to terrorists."

Another significant document is the Report that the United Nations Office on Drugs and Crime (UNODC) published in 2012, in Vienna. This Document aimed at helping and advising countries in the fight against '*terrorists'* using Internet (cyberterrorism) to plan attacks, to recruit and to make propaganda.

In respect of cyberterrorism as a Psychological Weapon in *Modern War*, Army corps general Fabio MINI, former commander of the General Staff of UN Command for South Europe, coordinator of *Comando Interforce for Balkan operations*, commander of UN peace operations in Kosovo-KFOR stated that: "*The war has changed, we can no longer be tributaries of the concept of traditional war when they shot each other. The war has changed not only because the people directly involved in this process and those collaterally interested are numerous, but especially because control systems are multiple: we no longer refer to traditional weapons, but to a multitudine of other types of weapons. A fundamental weapon of the modern war is the PSYCHOLOGICAL WEAPON, the weapon of influence being exerted on all and by all means, especially by computer, IT means […]. In 45 years of career, working all around the world, I have seen a lot of aspects that cannot even be described […]*"[4].

4. The notion of cyberterrorism

The concept / notion of cyberterrorism was certified for the first time in November 1794;

Initially, it defines the "*doctrine des partisans de la Terreur*", the doctrine of partisans of terror, representing the exercise of power by means of intense and violent struggle against those who acted and manifested against the revolutionaries – the French Revolution. It was a way of exercising power, not a way of acting against it, as defined today.

The term evolved during the nineteenth century and currently defines not a state action (the revolutionary state), but an action against it (terrorism). Its use, in anti-governmental respect, is attested in 1866 in Ireland and in 1883 in Russia (the nihilist movement-doctrine or attitude, based on denying all values, beliefs and opinions.

As François-Bernard Huyghe stated, "*Terrorism, in a modern sense, is born simultaneously with the emergence of current media institutions*"[5].

"*Criminal acts of political or other purposes intended or calculated to provoke a state of terror in the general public, from a group of persons, regardless of the reasons behind such political, philosophical, ideological, racial, ethnic, religious or any other kind are unjustifiable and condemnable*" (the United Nations).

4.1. Cyberterrorism – definition

"*Cyberterrorism*" is a controversial term, which is difficult to be defined, especially due to the lack of clear clarifications on terrorism itself.

Certain authors define it as being "*the multitude of attacks against information systems in order to destroy them and to generate a state of alarm and panic*". According to this limited definition, "*it is difficult to identify all actions and activities of cyberterrorism*".

As Kevin G. Coleman (*The Technolytics Institute*, article 6/23/2017) detailed, "*Premeditated actions / activities aimed at destabilizing information media / systems, with the intention of causing social, ideological, religious, political or any other kind of damage, with the ultimate goal of intimidating individuals or a group of individuals in order to force them or other groups / groups of individuals; to act / react in a certain sense*".

5. Cyberterrorism – the context of occurrence

The issue of cyberterrorism actually came into being with the events of September 11th, 2001, when the US administration announced it would implement a new defense strategy.

One month after the events of September 11th, 2011, US President George W. Bush signed *The Patriot Act*, *(i.e. "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001")*, the first global document that provides for legislation on terrorist activities[6].

The Patriot Act is an exceptional law the provisions of which initially extended for 4 (four) years. In July 2005, The American Congress permanently endorsed 14 of the 16 provisions.

After a long dispute, the American Congress, during the winter of 2005-2006, permanently endorsed most of the tasks assigned to the police and security forces.

Briefly, The USA Patriot Act:

- strengthens the power of government agencies– FBI, CIA, NSA and the army, thus reducing the right of defense;
- introduces the status of 'enemy combatant' and "*illegal combatant*";
- provides that any kind of intervention within an information system can be assimilated to a terrorist act;
- authorizes FBI to intercept all electronic messages and to preserve any trace of web navigation of persons suspected of terrorism or of contact with a

[4] Please see: www.libertaegiustizia.it;

[5] *Think tanks: Quand les idées changent vraiment le monde,Vuibert*, 2013;

[6] Amitai Etzioni, How Patriotic is the Patriot Act?:Freedom Versus Security in the Age of Terrorism, Routledge, 2004;

person suspected of terrorism;

- authorizes the phone interception of any person suspect of having close or distant links with a person suspected of terrorism. In August 2006, a federal judge found the inconvenience of telephone interceptions and ordered the cancellation of the secret interception program run by the National Security Agency (NSA).

Under these circumstances, associations for the protection of human rights started strong advertising campaigns on the consequences of the US Patriot Act, such as: attenuation of the right to defense or the violation of the right to privacy by authorizing electronic interceptions of any kind and telephone interceptions. They draw the attention on the risk of the agencies to interfere in the act of justice.

"*The problem is that all these derogatory procedures introduced in the name of the fight against terrorism have ended up by becoming rules. If they prove to be effective in combating this monster, which is the terrorism, therefore being used to fight against it in several areas, they have ended up contaminating the whole criminal law*"[7].

6. European Regulation. VIGIPIRATE

Starting with 2002, the European Union starts to issue framework decisions "*inviting*" Member States to adjust national legislation to the concept of prevention and fighting against terrorism.

For example, France adopted the VIGIPIRATE – an anti-terrorism plan drawn up in 1978 after the attack of Orly, of May 20th, 1978, and the taking of hostages at the Embassy of Iraq in Paris. The plan was completely rebuilt after the events of September 11th, 2001 and is continuously maintained at red level after the attacks of London.

VIGIPIRATE is a set of measures applied in any context and circumstances: *"…even in the absence of precise threat signals*".

In 2007, the latest version of VIGIPIRATE plan was released, founded on a clear principle: *"terrorist threat must be considered permanent"*. This instrument was updated in 2016.

In 2006, the Law on combating terrorism (LCT) presented by the Ministry of Foreign Affairs of the Republic of France, based on the articles of The USA Patriot Act, widen the obligation to preserve traffic data, even in case of '*cybercafés'*[8]

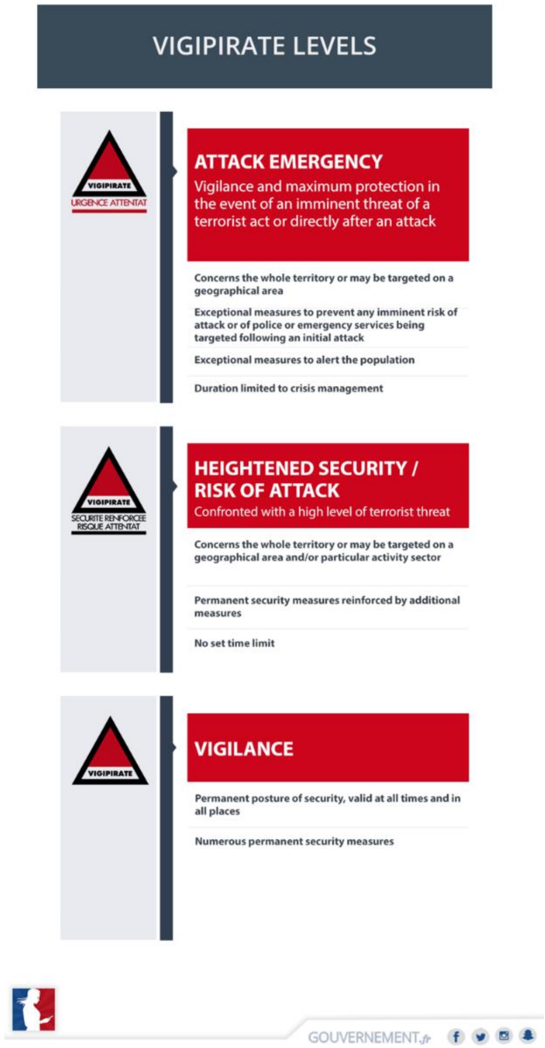
The law allows intelligence services operating in the field of preventing and combating terrorism to obtain access to the control of the information media – electronic surveillance – in the lack of a judicial authorization.

The surveillance on the internet is thus placed outside the judicial control.

VIGIPIRATE represented the source of inspiration for the European legislation in the field.

The amendments of 2014: widen the area of the operators involved – territorial communities and economic operators; decodes part of the plan of measures; restores the action plan[9].

Figure 1



VIGIPIRATE LEVELS

ATTACK EMERGENCY

Vigilance and maximum protection in the event of an imminent threat of a terrorist act or directly after an attack

Concerns the whole territory or may be targeted on a geographical area

Exceptional measures to prevent any imminent risk of attack or of police or emergency services being targeted following an initial attack

Exceptional measures to alert the population

Duration limited to crisis management

HEIGHTENED SECURITY / RISK OF ATTACK

Confronted with a high level of terrorist threat

Concerns the whole territory or may be targeted on a geographical area and/or particular activity sector

Permanent security measures reinforced by additional measures

No set time limit

VIGILANCE

Permanent posture of security, valid at all times and in all places

Numerous permanent security measures

Source: https://upload.wikimedia.org/wikipedia/commons/thumb/f/f0/Vigipirate-web-07_-_en.png/800px-Vigipirate-web-07_-_en.png

7. Regulations on prevention and combating terrorism in Romania

Terrorism offences are regulated, in the Romanian criminal law, by Law no. 535/2004 on the prevention and combating terrorism.

Such provisions are included in the current Criminal Code, in Title IV, as being the offences

[7] Christophe André, Maître de conférences à l'Université Versailles-Saint-Quentin (UVSQ). Il dispense également un cours de Droit de la répression à l'IEP de Paris;

[8] Tristan Nitot, Surveillance: Les libertés au défi du numériques:comprendre et agir;

[9] Please see: https://www.gouvernement.fr;

"*committed for the purpose of seriously disrupting public order, by intimidation, by terror or by creating a state of panic*".

As far as cyber space and its reference relations are concerned, the Romanian legislator did not at any time question the existence of terrorist actions.

The computer and the cyber media are considered by the lawmaker as simple instruments by which terrorist offences and acts can be committed.

The amendments of 2018 of Law no. 535/2004 refer to, *inter alia*, the notion of terroism: *"Terrorism is the ensemble of actions and/or threats that represent a public danger affect life, body integrity or human health, the ensemble of social relations, material factors, international relations of the states, national or international security, are politically, religiously or ideologically motivated and are committed for one of the following purposes: intimidating population or a segment of it, by producing a strong psychological impact, compelling a public authority or international organization to fulfill, not to fulfill or to refrain from the fulfillment of certain act, serious destabilization or destruction of fundamental political, constitutional, economic or social structures of a state or international organization".*

Terrorist propaganda materials are defined as follows: "*any material on hard copy, on audio, video media or other information data, as well as any other form of expression that makes the apology of terrorism or exposes or promotes ideas, concepts, doctrines or attitudes to support and promote terrorism or terrorism entity".*

The legislator provides the offences which are taken into account in this field, as follows:

a) the offences of homicide, second degree murder and first-degree murder, bodily injury and serious bodily injury, as well as illegal deprivation of freedom, all provided by the Criminal Code;
b) the offences provided by art. 106-109 of Government Ordinance no. 29/1997 on the Aerial Code, republished;
c) the offences of destruction provided by the Criminal Code;
d) the offences of non-observance of the regime of arm and ammunition, non-observance of the regime of nuclear materials and other radioactive matters, and of non-observance of the regime of explosives, provided by the Criminal Code;
e) production, acquisition, possession, transportation, supply or transfer to other persons, directly or indirectly, chemicals or biological arms, and research in this field or development of such arms;
f) introducing or spreading into the atmosphere, on the soil, into the subsoil, or into water, products, substances, materials, micro-organisms or toxins that are likely to jeopardize the health of persons or animals or the environment;
g) threatening with the commission of the acts in a)-f).

Other offences are provided by Articles 33-39 of the same law – offences assimilated with terrorist acts (Article 33), acts of terrorism committed on the board of ships or aircraft (Article 34), the deed of a person who leads a terrorist entity (Article 35), making available to a terrorist entity movable or immovable assets (Article 36), terrorist threats (Article 37) and terrorist alarming (Article 38), the administration of the assets belonging to a terrorist entity (Article 39).

8. Cyber Space Attacks

The main actions performed by ISIS, Al Qaeda and Hamas groups were mainly focused on propaganda, fundraising by cryptocurrency, as well as recruiting by social media and messaging applications (especially those protected by cryptography, such as *Telegram*);

If we analyze ISIS groups, these activities are declining, especially after the loss of '*capital'* Raqqa in Syria. Nevertheless, despite the forced abandonment of their neuralgic center for the production of information materials for propaganda purposes, the external communication of '*black flags'* was not completely disrupted, because of cells dispersion and their renewed autonomy allowed the maintenance of an operational continuity.

By analyzing action methods: *propaganda, fundraising and recruiting*, these are activities generally addressed to a mass audience and are therefore transmitted through the social media.

Nevertheless, Deep Web and Dark Web are spaces where certain actions are performed, such as such as the sale of arms – as in case of the attacks of Paris, in 2015.

Military equipment and materials pose a limited risk of being intercepted by the authorities on the internet. Jihadist terrorism, mentioned in the annual report of TIC presented by Eitan Azani, Deputy Executive Manager of the *International Institute for Combating Terrorism*, uses fundraising activities by means of cryptocurrency that guarantees the anonymity of the payer.

Several campaigns, such as Jahezona, of the Akhbar al-Muslim site or of Aaaq Foundation, remain alive and contribute to maintaining the work of the Islamic State.

The Isis-coins.com website invites users to change circulant currency on the territory of the caliphate – now dismantled – into virtual currency.

The existence of encrypted messaging applications facilitates communication: in addition to classical applications, some programmers who support Jihadists developed an encryption program called '*Muslim crypt'*, distributed by Telegram MuslimTech channel.

As far as the propaganda carried out in the *social media* is concerned, ISIS is committed to teach militants to protect online identity, as Bahaa Nasr, the manager of Lebanese project *Cyber Arab* explains.

The Justpaste.it platform provides manuals of the Caliphate in order to use Vpn (such as: http://justpaste.it/2ip); or advice collection on information security, from browser navigation to mobile phone (such as: http://justpaste.it/itt3).

The Global Islamic Media website uses source instruments and "*Islamize*" them: among them, an encrypted messaging program with Arabic and English tutorials.

ISIS has been lately focused on software and encryption programs for Android and Symbian that encrypts files, text messages, and emails.

Scott Terban, expert in cyber security and terrorism declared for '*Il Espresso'* that: "*Besides classical propaganda, the main IT activity of ISIS is to personalize such programs (encryption). Malware Hunters of Citizen Lab of the University of Toronto found in December evidence of the software delivered by e-mail to the anti-ISIS Syrian activists behind site «Raqqah is Slaughtered Silently». The program, if downloaded as a harmless attachment, can locate the victim. It is a rudimentary instrument, not as sophisticated as the one used by the pro-Assad Syrians (who have violated «Le Monde» Twitter profile by exploiting OpFrance visibility, but that are not part of the cyber jihad). ISIS is, therefore, the number one suspect"*.

In June 2017, hundreds of thousands of computers of Europe, America and Asia were hit by one of the most aggressive cyberattacks in history, performed by one of the most advanced malware programs ever created.

The scope of the hackers was above all the networks and systems of the medium and large companies including TNT, Reckit-Benkiser, Maersk and others. Hackers hit victim devices by using a redemption program, a program that, after infecting target computers, delete the entire content, unless the owner agrees to pay a redemption.

According to estimations, NotPetya (the name of the ransomware), costed companies more than EUR 1 billion, including the amounts paid and the damages caused to the production activities. NotPetya expands by exploiting a vulnerability in Windows operating systems: according to the investigations performed by ESET, the antivirus software manufacturer, the attack started in MEDoc servers, a program extended in Ukraine for the management of tax payments.

9. Forecasts

Ariel Levanon, vice-president of Cyber & Intelligence group stated that "*The challenge of Western intelligence agencies is not only to find terrorists, but to fully understand their capacity and motivation. Performing cyberattacks and transmitting messages over the Internet will, in fact, become more and more simple, with the increase in digitization of every aspect of life. At the same time, it will be more and more difficult to ensure the protection of the cyber space. It is expected that in the next five years, terrorist attacks in Western countries take place against the transport system and it is expected that an IT component support these attacks. There are no realistic solutions that do not take much time. It is essential to protect the information ecosystem by legal regulations, by the involvement of private companies, but above all, by teaching these problems in school*".

According to computer security experts, ransomware is one of the fastest cyberattacks to be multiplied in the future.

The European Union, by Directive 541/ 2017, included attacks against information systems in the category of "*terrorism offences*", by adopting a third legislative approach.

References

- Amitai Etzioni, *How Patriotic is the Patriot Act? Freedom Versus Security in the Age of Terrorism*, Routledge, 2004;
- Tristan Nitot, *Surveillance: Les libertés au défi du numériques:comprendre et agir*;
- Kenneth C. White, *Cyber-terrorism:Modern mayhem, U.S.Army War Colleg*e, 13 March 2015;
- http://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52017JC0450&from=EN);
- https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime;
- www.libertaegiustizia.it;
- https://upload.wikimedia.org/wikipedia/commons/thumb/f/f0/Vigipirate-web-07_-_en.png/800px-Vigipirate-web-07_-_en.png.