

***SUBJECT:** Conducted activities related to combating crimes against intellectual and industrial property rights on the Internet in 2019*

I. Situation analysis

1. Subjects of copyright or related rights whose rights are being violated and websites-offenders

1.1 Software products

Tracking and documenting of crimes against intellectual property related to software products becomes increasingly difficult because much of the products offered by the producer are delivered directly by them against the corresponding payment from the buyer's credit card online. At the same time fraudulent buyers provide their keys, passwords and product for use by third parties.

1.2 TV programs

There is an increasing trend in the supply and the use of the so-called set top box devices which provide access to TV programs through Internet connection across the globe using the technology IPTV (Internet Protocol Television) and the only thing necessary for the operation of those devices is internet access. This allows the user to watch TV literally anywhere with Internet access. These types of set top boxes are offered for sale **completely free** of charge including commercially available at large stores. For Bulgaria these imports come mainly from China. However to perform their function they need to be configured which is already carried out by persons and groups specialized in this field. It is to these persons and their actions to configure the devices and their secondary sale that criminal liability may be sought and realized for committed crimes under Art. 172A of the Penal Code of the Republic of Bulgaria, which states:

Section VII.

Crime against the intellectual property (Title, amend., SG 50/95)

Art. 172a. (New, SG 50/95) (1) (Amend., SG 62/97; amend. – SG 75/06, in force from 13.10.2006) Whosoever records, reproduces, circulates, broadcasts or transmits or uses in any other way another person's subject of copyright or related right or copies of it, without the consent of the proprietor of the respective right required by the law, shall be punished by imprisonment of up to five years and by a fine of up to five thousand levs.

(2) (Amend., SG 62/97; amend. – SG 75/06, in force from 13.10.2006) Whosoever keeps material carriers containing another person's subject of copyright or related right amounting to huge extent, or keeps a matrix for reproduction of such carriers, shall be punished by imprisonment of two to five years and a fine of two thousand to five thousand levs.

(3) (Amend., SG 62/97; amend. – SG 75/06, in force from 13.10.2006) If the act under para 1 and 2 has been committed again or substantial harmful consequences have been caused, the penalty shall be imprisonment of one to six years and a fine of three thousand to ten thousand levs.

(4) (new – SG 75/06, in force from 13.10.2006) In case the act under para 2 is in particularly large extent, the penalty shall be imprisonment of two to eight years and a fine of ten thousand to fifty thousand levs.

(5) (prev. text of para 4 - SG 75/06, in force from 13.10.2006) For minor cases the perpetrator shall be punished through administrative channels according to the Copyright and its related rights Act.

(6) (prev. text of para 5 - SG 75/06, in force from 13.10.2006) The subject of the crime shall be seized in favour of the state, irregardless of whose property it is, and shall be destroyed.

Art. 172b. (new – SG 75/06, in force from 13.10.2006) (1) Whosoever, without the consent of the owner of the exclusive right, uses in his/her commercial activity a trademark, industrial design, variety of a plant or breed of an animal, subject of this exclusive right, or uses a geographic name or its imitation without legal ground, shall be punished by imprisonment of up to five years and a fine of up to five thousand levs.

(2) In case the act under para 1 has been committed repeatedly or substantial harmful consequences have occurred, the penalty shall be imprisonment of five to eight years and a fine of five thousand to eight thousand levs.

(3) The subject of the crime shall be seized in favour of the state, irregardless whose property it is and shall be destroyed.

All this is done without the legal consent of the right holders of the television programs.

Another way of providing unauthorized access to TV programs is by offering the so-called. Android TV Box. Essentially they are hardware devices (minicomputers) that use the TV as a monitor and turn it into a Smart device. After connecting it and installing certain software product which most often is „Kodi Media Center‘ is gained access to multiple streaming servers physically located outside of Bulgaria which again provides illegal, unlimited and free access to a huge number of TV programs or movies.

The difficulty of investigating this type of illegal offering is resulted by the device's technology which is itself **not illegal** since it is a smart device like any phone, tablet or smart TV but how it is used to gain unauthorized access to TV programs is illegal.

1.3 E-books

There is a creation of groups on social networks /mainly Facebook/ whose members share and distribute non-regulated literary works in electronic form (Free eBooks, Electronic Community Centers etc.). More often in the country the social networks are also being used to carry on business activities with trademarked goods which violates the rights of the holders. A prerequisite for this trend is the widespread use of social networks for offering and communication and the relative anonymity of participants in it. According to Facebook as of January 2018 more than 4 000 000 Facebook profiles were administrated from the territory of Bulgaria. This in its essence reveals that Facebook is a major preferred social media outlet covering a fairly high percentage of the country's active population.

There are difficulties to counter this type of crime, having in mind that Facebook provides information mainly for crimes such as online child sexual exploitation and terrorism.

On the other hand identifying the perpetrators of those infringements of intellectual property rights is hindered by the lack of effective communication with global cloud service providers.

The systematic pressure of the Bulgarian authorities on sites that violate rights to literary works /https://chitanka.info/, led to their displacement on servers outside the territory of Bulgaria while others have stopped their activities /http://bookbg.net and more/.

Example:

Address lookup

canonical name	chitanka.info.
aliases	
addresses	104.27.153.167 104.27.152.167 2606:4700:30::681b:98a7 2606:4700:30::681b:99a7

Domain Whois record

Queried **whois.afiliias.info** with "chitanka.info"...

Domain Name: CHITANKA.INFO
Registry Domain ID: D20049292-LRMS
Registrar WHOIS Server:
Registrar URL: www.tucows.com
Updated Date: 2015-09-30T11:22:56Z
Creation Date: 2007-09-27T18:19:11Z
Registry Expiry Date: 2020-09-27T18:19:11Z
Registrar Registration Expiration Date:
Registrar: Tucows Domains Inc.
Registrar IANA ID: 69
Registrar Abuse Contact Email: domainabuse@tucows.com
Registrar Abuse Contact Phone: +1.4165350123

Reseller:

Domain Status: ok <https://icann.org/epp#ok>

Registrant Organization: Contact Privacy Inc. Customer 0133255543

Registrant State/Province: ON

Registrant Country: CA

Name Server: JADE.NS.CLOUDFLARE.COM

Name Server: BART.NS.CLOUDFLARE.COM

DNSSEC: unsigned

Network Whois record

Queried whois.arin.net with "n 104.27.153.167"...

NetRange: 104.16.0.0 - 104.31.255.255

CIDR: 104.16.0.0/12

NetName: CLOUDFLARENET

NetHandle: NET-104-16-0-0-1

Parent: NET104 (NET-104-0-0-0-0)

NetType: Direct Assignment

OriginAS: AS13335

Organization: Cloudflare, Inc. (CLOUD14)

RegDate: 2014-03-28

Updated: 2017-02-17

Comment: All Cloudflare abuse reporting can be done via
<https://www.cloudflare.com/abuse>

Ref: <https://rdap.arin.net/registry/ip/104.16.0.0>

OrgName: Cloudflare, Inc.

OrgId: CLOUD14

Address: 101 Townsend Street

City: San Francisco

StateProv: CA

PostalCode: 94107

Country: US

RegDate: 2010-07-09

Updated: 2018-10-10

Comment: All Cloudflare abuse reporting can be done via
<https://www.cloudflare.com/abuse>

Ref: <https://rdap.arin.net/registry/entity/CLOUD14>

1.4 Torrent websites

Unlike the large and well-established torrent trackers, the small ones are decreasing their popularity as a result of the systemic pressure and the permanent preventive measures of the officers from the Cybercrime Department within GDCOC. The large trackers try to cooperate with the right holders by unquestioningly removing the links (torrent files) for which they receive alerts from the right holders. This is a clear sign that they are trying to "legalize" part of their business by acting as suppliers within the meaning of the E - Commerce Act /ECA/. The main result of this pressure is the fact that no torrent website is officially hosted on servers in Bulgaria and it is worldwide known, that such sites in the country are considered illegal and their creation, maintenance and administration is prosecuted by the Bulgarian law enforcement agencies. To avoid the possibility of identifying the actual location of the site some of them use anonymizing open source services offered on Internet.

1.5 Streaming websites

With the development of Internet technologies and the improvement of digital infrastructure the creation of Internet sites operating on the principle of video streaming is becoming more and more common.

Video streaming or streaming media is a data transfer method commonly used for multimedia files. It is also known as **video streaming**/delivery (**live**) and the content that is transmitted in this way is commonly referred to as live video streaming.

In this case the streaming of content on the user's device begins with its access without having to download the file first and then start in a suitable player. Data transmission is simultaneous with the streaming so constant network connectivity is required.

Most commonly these types of sites are used to provide users with access to video /movies/, television or radio programs /live streaming/.

In analyzing the criminal scheme for providing access to subjects of copyright or related rights through these types of sites it was established that the perpetrators */mainly foreign nationals /* often create websites with the help of site creation platforms, host them outside the country or in the country by hiding their location through available anonymization resources on the Internet such as the service provided by the US company Cloudflare. Practice shows that streaming servers are not configured and activated in Bulgaria but already available ones that are positioned in the infrastructure of suppliers mainly from France, Germany, the United Kingdom and Romania are used.

2. Anonymization

A common way to anonymize is to move illegal servers on a „cloud“. Criminal structures are looking for ways to disguise the Internet crime perpetrators where there are many resources available to do so. In order to hinder and slow down the work of the Bulgarian law enforcement agencies usually websites or other resources are deployed on servers abroad or „in the cloud“. This avoids the possibility of documenting by standard methods the criminal activity because concepts such as "place of action" and "place of completion" are not relevant to the nature of the "cloud services" provided.

Introduced by the EU GDPR new rules on data listed in WHOIS registers provide web offenders with the same anonymity which is also offered by world leaders in anonymous hosting services such as Contactprivacy.com, Namecheap.com, Privacyprotect.org and others within US jurisdiction. The GDCOC practice on Internet crime investigation shows that the domain name anonymization services are used predominantly by offenders or law abusers who in order to make identification more difficult erase their traces of their illegal activity. This is the presumption with which the Bulgarian legislation introduces requirements that should be observed by site owners located on the territory of the country.

Essentially they are providers of electronic public services and their activity is regulated by the E – Commerce Act where in Article 4, Paragraph 1 is said that they must provide the recipients of the services and the competent authorities with unobstructed, direct and permanent access to certain information - their name, permanent address or registered office, address where it operates if different, correspondence details /telephone and e-mail address / for direct and timely communication with him and others.

What should be noted is that if the activities of these providers do not contradict the law then these requirements are met. If the activity carried out through the site is illegal then this information is not described in it and the only possibility to identify the crime perpetrator remains to consult the public Internet domain registers. They as a result of the implemented EU GDPR rules do not provide such information.

In summary it can be concluded that these rules do not prevent the identification of the crime as such but prevent the identification of the offender and help him/her to avoid criminal liability.

Another way to cover up the perpetrator`s identity is to use the services of the US company CloudFlare which conceals the actual location of incriminated Internet resources on a site-by-site scheme.

Analysis of the most popular torrent sites for 2019 shows that most use the CloudFlare service to cover up the actual location of the incriminated webpage.

Top 10 Most Popular Torrent Sites of 2019

№	WEBSITE	DOMAIN REGISTER	IP ADDRESS	HOSTING	C
1.	https://yts.am/	internet.am-Armenia	104.27.215.28 104.27.214.28	Cloudflare, Inc.	U
2.	https://1337x.to/	No data	104.31.17.3 104.31.16.3 2606:4700:30::681f:1103 2606:4700:30::681f:1003	Cloudflare, Inc.	U
3.	https://thepiratebay.org/	easydns.com-Canada	104.27.216.28 104.27.217.28 2606:4700:20::681b:d81c 2606:4700:20::681b:d91c	Cloudflare, Inc.	U

4.	http://rarbg.to/index70.php	No data	185.37.100.122	NETSAAP_BOSNIA	B H
5.	https://torrentz2.eu/	PrivActually Ltd-Cyprus	104.31.18.30 104.31.19.30 2606:4700:30::681f:131e 2606:4700:30::681f:121e	Cloudflare, Inc.	U
6.	https://nyaa.si/	domene.si	185.178.208.182	DDOS-GUARD- NET208	R
7.	https://www.limetorrents.info/	namecheap.com- USA	104.27.209.30 104.27.208.30 2606:4700:20::681b:d11e 2606:4700:20::681b:d01e	Cloudflare, Inc.	U
8.	https://zooqle.com/	easydns.com- Canada	104.25.203.13 104.25.202.13 2606:4700:20::6819:cb0d 2606:4700:20::6819:ca0d	Cloudflare, Inc.	U
9.	https://eztv.io/	gandi.net-France	104.25.47.104 104.25.48.104	Cloudflare, Inc.	U
10	https://www.torrentdownloads.me	namecheap.com- USA	104.27.212.30 104.27.213.30 2606:4700:20::681b:d51e 2606:4700:20::681b:d41e	Cloudflare, Inc.	U

The analysis of the most popular torrent sites in Bulgaria confirms this trend.

The lack of the ability urgently to obtain detailed data for both the location and the user of the CloudFlare service does not allow the continuation of the case investigation, given the fact that, if received by the provider is often insufficient or outdated.

Thus a service that by its very nature seeks to intercept the DDoS attacks against legitimate websites is used to disguise the location of websites that violate the law.

Top 10 Most Popular Bulgarian Torrent Sites of 2019

№	Site	IP address	Hosting	State
1.	http://zamunda.net/	179.43.173.102	Private Layer Inc	Panama
2.	http://zelka.org/	141.255.162.82	Clientid7747	Panama
3.	https://arenabg.com/	179.43.145.233	Private Layer Inc	Panama
4.	http://p2pbg.com	85.25.198.116	Host Europe GmbH	Germany
5.	http://alein.org	94.242.254.120	Root Sa	Luxemburg
6.	http://energy-torrent.com	104.24.108.207 2400:cb00:2048:1::6818:6ccf	Cloudflare	USA
7.	http://masters-tb.com	188.138.91.212	Host Europe GmbH	USA
8.	http://data-bg.net/	104.18.62.59	Cloudflare	USA
9.	http://www.avetorrents.com/	104.27.166.165	Cloudflare	USA
10	http://torrent-team.net/	115.146.127.253	CMCTELECOM	Vietnam

Law enforcement authorities are increasingly required to collect and use electronic evidence which, in the formal proceedings of the Bulgarian investigation, remains indirect or misunderstood.

3. Legislation

A major obstacle investigating this type of crime is the legislative qualification as a minor offense - sentence of up to 5 years' imprisonment. This, on the one hand, hinders the use of special investigative means and, on the other, the collection of elementary electronic evidence, which by its very nature requires access to the so-called 'traffic data' which, according to The Electronic Communications Act, is provided to the authorities only after a judicial authorization, and only in the presence of a serious deliberate crime - one for which a term of imprisonment of more than 5 years is provided.

Although the means and the medium of implementation of the crime happen in the cyber space, the existing legislation in Bulgaria (E - Commerce Act, Electronic Communications

Act, ZEDP) does not regulate the responsibility of the provider of the respective service, as well as the procedure for storing and receiving the information needed to identify the mechanism and the perpetrator of the crime.

On the other hand, the E - Commerce Act regulates the activity of the providers of specific services on the Internet (linking and hosting). Accordingly, these providers are not obliged to retain the computer data - necessary data for the identification of a particular perpetrator of a crime. The Act states that the providers of these services are obliged to provide all information about the users of certain services, but there is no explicit regulation regarding the way they are provided, due to the fact, the data is not maintained.

Intellectual property crimes are acts of high public danger, not only in the light of the rights and in the light of interests of the individual author concerned, but also in the interests of the state related to the affirmation of national identity, which is formed by the creative guild of our nation.

In connection with the above, in July 2019 a proposal was made by the Cybercrime Department at the General Directorate Combating Organized Crime to change the texts of the Penal Code of the Republic of Bulgaria. The changes concern an increase in the amount of penalties under Art. 172A and 172B, as well as all paragraphs of Chapter IXA of the PC.

If the sentence of imprisonment is increased for more than 6 years, these crimes will become serious and this will allow the authorities of GDCOC to:

1. Collection of especially important electronic evidence for investigations - representing "traffic data" required only for serious premeditated crime through judicial sanction;
2. The use of special investigative means according to the Special Investigative Means Act: wiretapping, surveillance, controlled delivery, etc.

II. Actions and administrative reforms undertaken by the Ministry of the Interior within the structure of the General Directorate Combating Organised Crime (GDCOC)

1. Increasing the administrative capacity of the GDCOC

On March 14, 2018, under the sanction of the Minister of the Ministry of Interior Mladen Marinov, Cybercrime Unit at GDCOC (with 16 staff members), which was established in 1998 having 16 officers in its structure was transformed into Department with 40 officers, divided into 3 Units: Cyberattack Unit (14 officers), Illegal Content on the Internet (13 officers), and Digital Analysis and Open Sources (10 employees).

Intellectual property offenses are within the purview of Illegal Content on the Internet Unit, which is completed with all vacancies only in early 2019 and 7 officer work in the Intellectual Property field.

2. Establishment of a National Contact Point for the Ministry of Interior under the Intellectual Property Line in the newly formed Unit “Illegal Content on the Internet”

At the beginning of 2019, it was identified that the Illegal Content on the Internet Unit had to be designated as a contact point of the MoI at national level, regarding Europol, the EU Intellectual Property Office (EUIPO), as and the US law enforcement agencies in the area of Intellectual and Industrial Property. The same happens on 08/02/2019 by virtue of a proposal approved by the Chief Secretary of the Ministry of the Interior Ivaylo Ivanov to the GDCOC Director, number 1266p-3037/ 06/02/2019 and the followed commandment of the Secretary General of the Ministry of the Interior number 8121p-2855/08/02/2019.

The purpose of creating this contact point is to contribute to the collection, analysis and compilation of data relating to the actions taken by the Ministry of the Interior at national level to counteract intellectual and industrial property crime, in order to achieve an overall picture of the activities of MoI. This data is provided by the 28 regional structures of the Ministry of the Interior in the country every month to the Illegal Content on the Internet Unit, and after being summarized the data is directed to the online platforms of Europol and the EU Intellectual Property Office / EUIPO /: www.ipenforcementportal.eu.

Outcomes after the establishment of the National Contact Point in the field of Intellectual and Industrial Property up to September 2019

A. Data received from the MoI structural units for pre-trial proceedings initiated from February 2019 to date concerning Intellectual Property.

MoI Structure	Pre-trial proceedings under article 172 of Penal Code	Pre-trial proceedings under article 172b of Penal Code
Directorate General Border Police	-	21
Sofia Metropolitan Police	1	20
Varna Regional Police Directorate	-	12
Burgas Regional Police Directorate	-	15
Plovdiv Regional Police Directorate	-	1
Shumen Regional Police Directorate	-	1
Pazardzhik Regional Police Directorate	-	2
Lovech Regional Police Directorate	-	1
Sliven Regional Police Directorate	-	2
Vidin Regional Police Directorate	-	6
Pre-trial proceedings in total for 2019	1	81

The analysis of the collected data shows that by 09/2019 the structural units of the Ministry of Interior had worked out and reported to the competent prosecutor's office mainly signals of committed crimes under 172b of Penal Code, mainly by Directorate General Border Police, which is probably due to the fact that their powers are exercised in risk areas where multiple offenses against intellectual property are committed. Such activities are detected in the border regions (Vidin), the areas with enhanced international transport links, and resort areas (Sofia, Varna and Burgas).

B. Data regarding conducted operations by the Illegal Content on the Internet Unit in 2019, in the field of Intellectual Property

	Under article 172 of Penal Code	Under article 172b of Penal Code	Total
Formed Pre-trial proceedings up to			

September 2019	10	5	15
Executed specialized police operations	14		14
Filed up signals	248		248
Aborted violations of individual rights	13450		18016
Closed illegal sites	110		110

The analysis of the results shows a significant increase in indicators compared to those in 2018. For example:

- The pre-trial proceedings initiated under art. 172a of the PC for 2018 are 4 in the case of 10 for 2019
- The pre-trial proceedings initiated under art. 172b of the PC for 2018 are 4 in the case of 5 for 2019
- The specialized police operations conducted for 2018 are 10 the case of 14 conducted in the first months of 2019
- Access to 12500 individual violations suspended for 2018 compare to 18016 for the 2019
- In 2019, access to 110 Internet sites through which intellectual property crimes were committed was suspended

III. Counteraction operations carried out by the DGCOC Cybercrime Department in 2019

1. On 07/02/2019, officers from the Illegal Content on the Internet Unit at DGCOC have taken actions to investigate four addresses in the city of Varna, where numerous textiles, sports goods and perfumes were found and seized, totaling more than 10,500 items branded Louis Wooton, Dolce and Gabbana, Carolina Herrera, Paco Raban, Diesel, Hermes, Azaro, Valentino, Chanel, Versace, Gucci.

In addition, three laptops were seized from which Internet goods sales were administered, over 100 perfumes, over 100 wallets, over 500 sunglasses, over BGN 17 thousand, more than 50 men's handbags, more than 100 sunglasses, documentation regarding the criminal activities, two mobile phones, 2 laptops.

Access to the following 15 sites distributing counterfeit goods to consumers in Bulgaria, Greece and Romania has been suspended: ww.estilno.com, www.kecmania.com, www.fashionbg.net, www.fashionhit.net, www.perfumegr.com, www.aromagr.net, www.ukperfume.net, www.aromamea.com, www.aromatbg.net, www.perfumebg.net,

www.hitochila.com, www.outletshop.biz, www.perfumero.net, www.stararoma.net and www.zonadebarbati.com

Two persons were detained. In carrying out the operational inspection by National Revenue Agency (NRA) officers, huge turnovers were detected which were not fiscalized. After summarizing the information collected, it has been clarified that the damage to the fiscal account was particularly large.

It has been found that more than 10 persons with different functions are involved, working entirely in the gray economy. To companies and individuals have been assigned financial audits to document crimes under Art. 255 of the Penal Code of the Republic of Bulgaria.

Based on the quantity of goods seized, the damage inflicted amounted to over BGN 1.7 million, excluding the realized profits, which will be reported by the NRA

2. On March 13, 2019, on the territory of Blagoevgrad district, officers from the Illegal Content on the Internet Unit was conducted an operation countering online distribution of a foreign trademark. In the course of the operation, the activity of **17 websites** hosted on the territory of the Republic of Bulgaria, carrying out online illegal trade in goods, objects of trademarks were suspended. The sites are as follows: www.vipdirect.net, <http://allbrands.eu/>, <https://big-style.eu/>, <http://dressdirect.eu/>, <http://vzemisi.eu/>, <https://outletzona.net/>, <http://ekipi.eu/>, <http://modamorado.com/>, <https://drehi.site/>, <https://reflex.bg/>, <http://outlet-365.net/>, <https://magazindrehi.online/>, <http://baza1.eu/>, <http://aromani.eu/>, <https://dresdirect.net/>, <https://drehizanego.com/>, <http://ekipi.net/>

In the course of the operation, the a factory for the production of garments bearing the distinctive signs of brands BOSS, DOLCE GABBANA and others was dismantled. It was found and seized from the perpetrator's vehicle a total of 14 various articles of registered trademarks, empty polyethylene envelopes of a courier company, prepared consignment notes, cloth top, various notes and goods receipts. From the office of the courier company were seized 3 consignments containing sporting goods from the brands G Star Raw Denim and Hugo Boss. Nokia mobile phone used by the perpetrator was also seized. Operational activities were performed at two addresses in Blagoevgrad. One of them has 3 /three/ premises with many goods from registered trademarks. The first room is also suitable as a photo studio with two professional umbrella lamps. At the address are found many textiles - jeans, sportswear, T-shirts, etc., sunglasses, hats and more. In addition, 4 laptops, 2 desktops, 3 mobile phones that were contacted on the sites, multiple bills of lading, 2 fiscal devices were seized. The premises accommodate employees who dealt directly with online commerce

and order processing from a total of 15 / fifteen / sites. In a house located at the entrance of Pokrovnik village, a shop for the production of goods was established, and machines for branding, cutting and stamping of textile products were found and seized. In the house are found many labels with the logo of world famous brands: Boss, Armani, Nike, G - Star, Dolce & Gabbana, Louis Vitton, Sport Plein, Gucci, Adidas, billets and finished products. Two persons found to be directly involved in the production and distribution activities were detained. The damage done to the fiscal and the right holders is enormous. Revisions are made by the NRA for documentation purposes.

3. On June 13, 2019, eight teams of cybercrime officers at GDCOC, experts from the Europol Intellectual Property Unit, teams from the Gendarmerie Directorate, NRA officers and officials of the Communications Regulation Commission conducted coordinated specialized police operations on the territory of three districts in the country. Investigations were carried out at the premises of four cable operators broadcasting television programs in the cities of Kyustendil, Dupnitsa, Gotse Delchev, Sandanski, Petrich, Kardzhali and Burgas, without the legal consent of the right holders, according to which the damage caused by the illegal activities are for over ten million BGN. The operations have documented a number of offenses committed by the managers of companies that violate the law. In one case, an Internet service provider operating in the territory of Sandanski was found to have even created an Internet and mobile application, thereby providing unregulated access to consumers to more than 150 television programs without the legal consent of the right holders. During the operations carried out, a large number of equipment was seized by which the criminal activity was carried out - server systems, online streaming configuration, decoders, modulators, digital amplifiers, signal testers and more. The anti-piracy operation is one of the largest in Europe, according to representatives of the Europol Intellectual Property Crime Center.

4. On August 6, 2019, a 44-year-old person was detained by officers of the Illegal Content on the Internet Unit in cooperation with the Sofia District Prosecutor's Office. According to initial data, the man has created and administered over 40 websites, through which he distributed on the Internet current film works. He originally published the films on one of the sites he controlled. After reaching a certain number of visitors and the traffic generated, for which he was paid for by Google, he downloaded the works and shared them again, but in some other domains. The procedure was repeated 4-5 times until the resource

was exhausted from the sites it controlled. Thus, for the same copyright sites, he received multiple payments from Google, as it involved internet traffic to different domains. Access to the websites used for criminal activity - www.x-movies-8.com, www.new123movies.com, www.phim-3s.com, www.phim-14s.com, www.xxxmovies8.com, www.wwl1.serialitebg.com, www.xmovies8-tv.com, www.onlinemovies2017.com, www.www1.xmovies-8.com, www.onlinemovies2016.com, www.newcinema2016.info, www.movies-16.com, www.onlinemovies-gold.com, www.megashare-movies.com, www.newmovies-2016.com, www.onlinemovies-is.com, www.big-top-40.com, www.movie-8k.com, www.tv-1000.net, www.online-movies-pro.info, www.moviesonline-pro.com, www.filmi-bg-audio.com, www.terminator-genesys-online.info, www.starwars7-download.info, www.resident-evil-7-online.info, www.mision-impossible-5-online.info, www.james-bond-24-online.info, www.onlain-filmi-bg.com, www.filmi-fen.com, www.filmi-2015.com, www.kinofilme-2014.com, www.movies-2017.com, www.hulu-movies.com, www.onlain-filmi.info, www.wwl1.movies-2015.com, www.movies-16.com, www.movie-32.com, www.new123movies.stream/cgi-sys/suspendedpage.cgi, was suspended within the framework of the investigative actions, collecting the necessary electronic evidence. Most sites were hosted on the Internet by one of the largest international cloud service providers in the United States. This led to the impression of the perpetrator that he remained anonymous, but an international investigation documented his criminal activity to an end.

5. On September 18, 2019, an international operation was carried out simultaneously on the territories of the countries concerned, in order to document the activities of OCGs engaged in the illegal distribution of television channels throughout Europe by officers of the "Illegal Content" Unit, Eurojust / EU Judicial Cooperation Body /, partner services from Italy, Germany, Greece, France, the Netherlands and Spain. The international investigation revealed that the company operating the popular IPTV management system Xtream Codes, provides up to more than 5,000 suppliers / resellers /, which in turn provide unregulated access to over 50,000,000 end-customers. On the Bulgarian territory, pursuant to European Investigation Orders (EIOs) from Italy, investigations were carried out at 2 addresses in Petrich. Documents related to the illegal activity and three hard drives were found and seized. More than 200 servers in the address space of Germany, France and the Netherlands have been discontinued and over 150 PayPal accounts used by criminals have been suspended. The damage caused by

the criminal group amounts to approximately € 6.5 million, jeopardizing the existence of many legitimate pay-TV providers in the market.

The international operation executed on 18.09.2019 is a result and a continuation of the International Operation NOVA, executed on 09.01.2018, by Europol, Cybercrime Department at GDCOC, the Cypriot, Greek and Dutch partner services, simultaneously in the territories of Bulgaria, Cyprus, Greece and the Netherlands, in order to document the activities of OCGs engaged in the illegal distribution of television channels throughout Europe. On Bulgarian soil, pursuant to a Legal Aid Request (IPA) from Cyprus, investigations were carried out at 4 addresses (2 each in the cities of Sofia and Petrich). Found and seized were 84 servers, a set top boxed MAG device (receiver), 70 satellite receivers, 5 converters for video to digital signal conversion, remote control systems, network equipment, computer configurations and documents. A 47-year-old Greek citizen was detained for up to 24 hours. 10 witnesses were interviewed and 5 persons were identified by photos. In Cyprus, searches were carried out at 9 addresses and servers and other equipment were seized, and 4 persons were detained. There have been 4 searches in Greece, no detainees. There was 1 search in the Netherlands. As a result of the operation, the illegal broadcasting of over 100 television channels across Europe has been stopped.

6. On 21/01/2020, officers from the "Illegal Content on the Internet" Sector at the Cybercrime Department of the GDCOC, officers from the team in the cities of Haskovo and Kardzhali, teams of the Gendarmerie Directorate, employees of National agency of income, employees of the Communications Regulation Commission and the Ministry of Culture, conducted an inspection and an investigation in the office of Internet provider "Technolux" Ltd. with UIC 108692434, Kardzhali.

The inspection was related to a pre-trial proceeding with the number 307/2019 by the inventory of GDCOC.

A preliminary check by the officers of the „Illegal Content on the Internet“ sector at the Cybercrime Department revealed that the Internet provider provides access to more than 30 television programs to its clients without the legal consent of the right holder.

The operator has not declared providing television programs to end users in its activity, which is required by law.

During the search and seizure process at the address city of Kardzhali, 27 Bulair Street - office of the company Technolux OOD, a number of documents were found and seized at the address, related to the fact that the company is providing TV channels. Collaboration

agreements have been established between Technolux OOD and Global Communication TV Ltd for providing television programs to end users of the Internet service provider. About 10 contracts between end-users and Global Communication TV EOOD were found, as well as a database of about 1,700 subscribers. Ascertaining minutes were drawn up for the inspections carried out by the employees of the Ministry of Culture, the Communications Regulation Commission and the National Revenue Agency. Ascertaining protocols have been drawn up for the checks carried out by the representatives of the National agency of income, the Communications Regulation Commission and the Ministry of Culture.

7. On 21/01/2020, officers from the "Illegal Content on the Internet" Sector at the Cybercrime Department of the GDCOC, officers from the team in the cities of Haskovo and Kardzhali, teams of the Gendarmerie Directorate, employees of National agency of income, employees of the Communications Regulation Commission and the Ministry of Culture, conducted an inspection and an investigation in the office of Internet provider Netronix Ltd. with UIC 200907932, Kardzhali.

The inspection was related to a pre-trial proceeding with the number 3/2019 by the inventory of Sector Combating Organized Crime-Kardzjali.

A preliminary check by the officers of the „Illegal Content on the Internet“ sector at the Cybercrime Department revealed that the Internet provider provides access to more than 20 television programs to its clients without the legal consent of the right holder.

The operator has not declared providing television programs to end users in its activity, which is required by law.

During the search and seizure process at the address city of Kardzhali, 94 Bulgaria Blvd. - office of the company Netronix Ltd, a number of documents were found and seized at the address, related to the fact that the company is providing TV channels.

Joint venture contracts between Netronix Ltd and Global Communication TV Ltd, about providing television programs to end users of the Internet service provider, were seized.

Discrepancies in the contracts between end-users and Global Communication TV EOOD were found, as well as a database of about 4,500 subscribers. Ascertaining protocols have been drawn up for the checks carried out by the representatives of the National agency of income, the Communications Regulation Commission and the Ministry of Culture.

IV. Interaction with legal entities in the country

The GDCOC's Cybercrime Department is active in communication and cooperation in countering intellectual and industrial property crime with the private sector. Such companies are Aris Consulting, Turku Tager and Turku Law Firm, Association of Television Program Providers, BAPTO and others. DGCOOC staff takes part in seminars and meetings with the aforementioned companies, representatives of the private sector, which helps to gain valuable experience and build opportunities for cooperation in the fight against intellectual property crime.

In May 2019 GDBOP employees attended an annual meeting of the Association of Broadcasters.

On October 17-18, DGCOOC staff were attending a seminar organized by Turku, Tager and Turku, which is attended by representatives of Toyota, STIHL, PUMA, HP, Western Digital, SANDISK, POLO, LOREAL, CHANEL, COTY, HUGO BOSS, BAUER, LVHM PERFUMES, MOBIS, HONDA, HARLEY-DAVIDSON, BIO-OIL, JBL, SHISEIDO, SAMSUNG, ADIDAS, DIAGEO, FILA, DANIEL WELLINGTON, HASBRO, MCM. On the initiative of DGCOOC, an invitation was also sent to US Customs and Border Protection Attaché Mr. Douglas E. Eckhardt.

V. Forthcoming actions:

1. GDCOC has received a complaint from the publishers "BARD" Ltd., UIC 040760356, represented by the manager Anelia Nikolova Andonova, through the legal counsel Neno Dimitrov Nenov. The complaint is about an unauthorized distribution of works of art on the Internet through the site www.spiralata.net. The established works of art in Bulgarian language, on which "BARD" Ltd. has exclusive copyrights and are distributed on the site www.spiralata.net are written by authors such as Michio Kaku; Marie Kondo; Stephen Hawking; Deepak Chopra; Erih Fon Deniken; Susan Forward; Clarissa Pinkola Estes; James Redfield; Sergey Filonov.

Contracts were applied with the complaint for the distribution of the books by BARD Ltd., also screenshots showing the possibility of accessing the contents of the books, as well as a CD with all the contents of the listed books.

After interrogating Neno Dimtrov Nenov, it is confirmed that there is illegal publishing and distribution of the books for which the BARD publisher has exclusive rights in the territory of the Republic of Bulgaria.

Nenov stated that BARD Ltd. did not grant any rights for such distribution and was not asked by representatives of the website www.spiralata.net for the settlement of such.

The website www.spiralata.net is associated with the IP address 79.98.109.190, which is part of the address space of DELTA SoftMedia Ltd., which is physically located in Sofia.

Related to that, a request was sent to the company DELTA SoftMedia Ltd. about all the available information about the owner of the site. From the received response it became clear that the user of the server with IP address 79.98.109.190, which is hosted by www.spiralata.net, Ognyan Mladenov Ivanov, manager of the company "Seom" Ltd., UIC 201343922. The service is paid through six-monthly payments through the ePay.bg system.

The materials were sent to the Sofia District Prosecutor's Office. Pre-trial proceedings have been initiated with the number 427/2019. Investigation actions are forthcoming.

2. At the end of 2019 checks have been carried out about 6 cable operators, operating in different regions of the country which are providing their users with access to television programs without the legal consent of the right holders. After completion of the inspections, the materials were reported to the Supreme Court of Cassation for pre-trial proceedings. On 01/28/2020 a coordination meeting was held at the Supreme Court of Cassation to discuss the conduct of an operation against the activities of the six companies. The operation is expected to take place by the end of February 2020, with the participation of officers from the Cybercrime Department, representatives of the National agency of income, the Communications Regulation Commission, the Ministry of Culture and the Gendarmerie Directorate.

3. A training is planned for the officers of the Cybercrime Department and for representatives of the Prosecutor's Office of the Republic of Bulgaria about counteracting crimes and infringements related to intellectual property and Internet. The training will take place at the end of March 2020. and will be led by representatives of the Audiovisual Anti-Piracy Alliance (AAPA).

VI. Cooperation with foreign law enforcement agencies

In October 2019 representatives from different Bulgarian authorities were on a business travel in USA. The main purpose were meetings with leading business organizations and governmental authorities, which are responsible for the combating with the crimes against intellectual property crimes, copy rights and related rights.

Participants from Bulgaria were:

Commissioner Yavor Kolev – head of department “Cybercrime” part of General Directorate Combating Organized Crime and National Coordinator for Cyber security in Republic of Bulgaria

Chief inspector Mihail Dragodanov – head of sector “Illegal content on the Internet” part of General Directorate Combating Organized Crime

The chief prosecutor’s spokesman of Republic of Bulgaria - ms. Rumyana Arnaudova
Mr. Mehti Melikov – Director of directorate Copyrights and related rights, part of Ministry of Culture.

Chief inspector Ivelina Troshanova – head of sector “Financial crimes” part of General Directorate National Police.

During the meeting with Mat Lamberti an agreement was reached that an MLAT will be sent by our country, regarding initiated pre-trials concerning four torrent trackers – with the aim of seizing domains, registered in the USA:

Zamunda.net

Arenabg.com

Rarbg.to

Zelka.org

In General Directorate Combating Organized Crime were received four complaints from the organization Terapro – organization for protection of the legal distribution of TV channels. the short future is planned to report all collected data to Supreme Prosecutor office. The inspection on our part is complete and a report to the Supreme Prosecutor's Office is forthcoming. When the pre-trials will be initiated, MLATs will be sent to the USA’s law enforcements.

In case of successful actions and seizing of the mentioned domains, another MLATs will be sent to other countries, where other mirror domains are registered.

