МІЖНАРОДНІ ЧИТАННЯ
з міжнародного права
пам’яті професора
П.Є. КАЗАНСЬКОГО

МАТЕРІАЛИ
третьої міжнародної наукової конференції

До 15-річчя
Національного університету
«Одеська юридична академія»

Одеса, Україна
2-3 листопада 2012

Одеса
Фенікс
2012

THE TRANSNATIONAL DIMENSION OF CYBERCRIME

Nowadays the number of crimes which are connected with computers is increasing instantly due to the rapid development of information technologies. That is why with the creation of international
computer networks it is extremely important to make steps towards the international cooperation and coordination in this area. The transnational nature of crimes with a use of computer networks gives a reason to consider that the development of a common policy on such major issues must be a part of strategy to fight against any crime.

There are no doubts that computer crimes like all other types of illegal activity carry out the considerable threat to people, state and society. Moreover with the appearance of such crimes the extent of such threat is not yet fully understood. But the experience of the most developed countries in the world clearly shows the undeniable vulnerability of any state. Since the computer crimes do not recognize any borders it is understood that any criminal is equally capable of threatening information systems which are located all over the world.

Computer crimes as a rule are much more complicated than «usual» crimes. And it is not rare that computer crimes go far out of the framework of the current legislation. There is also a problem concerning the detection of crimes. Usually, the traces are erased or destroyed. Another feature of computer crimes which is even much more difficult for detection is the use of satellite systems, so that such crimes can be committed at a significant distance from the object of the crime in a short period of time. But the investigation of such crimes can take weeks or even months allowing criminals to destroy evidences of a crime which gives them an opportunity to avoid punishment.

To prevent and fight against cybercrime effectively the coordinated approach is needed at different levels. At the national level to investigate such crimes a well-trained, professional, competent and qualified staff is required. Also, it is necessary to make amendments and additions to the existing national legislation in order to create the legal basis for the law enforcement bodies to work more successfully and for the judiciary — to the offenses in the field of information, including the suppression of transnational computer crimes. At the international level for cybercrime investigations require speedy actions based on the coordination of national law enforcement bodies for the prevention and investigation of transnational computer crimes with similar international bodies in other countries.

To solve the problems at those levels it is necessary to set up a legal definition of the most important standards of conduct of the participants fighting against offenses related to the use of the Internet.
Criminal policy of separate state in the sphere of fighting transnational cybercrime has a direct impact on the international community in the scope of fighting the crimes which is committed with the use of global computer network (Internet). Cybercriminals can act in a certain state, where such conduct is not criminalized, so they can be protected by the law of that country. Even if the legislation of the specific national interests of a state is not included the criminalization of certain acts, it may consider adopting such measures, in order not to be in a stance of international isolation. It is impossible to fight transnational cybercrime without the unification of the criminal legislation of the international community.

The United Nations Convention against Transnational Organized Crime, adopted by General Assembly resolution 55/25 of 15 November 2000, is the main international instrument in the fight against transnational organized crime. It opened for signature by Member States at a High-level Political Conference convened for that purpose in Palermo, Italy, on 12-15 December 2000 and entered into force on 29 September 2003. The Convention is further supplemented by three Protocols, which target specific areas and manifestations of organized crime: the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children; the Protocol against the Smuggling of Migrants by Land, Sea and Air; and the Protocol against the Illicit Manufacturing of and Trafficking in Firearms, their Parts and Components and Ammunition. Countries must become parties to the Convention itself before they can become parties to any of the Protocols.

The Convention represents a major step forward in the fight against transnational organized crime and signifies the recognition by Member States of the seriousness of the problems posed by it, as well as the need to foster and enhance close international cooperation in order to tackle those problems. States that ratify this instrument commit themselves to taking a series of measures against transnational organized crime, including the creation of domestic criminal offences (participation in an organized criminal group, money laundering, corruption and obstruction of justice); the adoption of new and sweeping frameworks for extradition, mutual legal assistance and law enforcement cooperation; and the promotion of training and technical assistance for building or upgrading the necessary capacity of national authorities.
The UN Convention against Transnational Organized Crime is the major step to fight and prevent the transnational crimes and their consequences. It contains the general notions, provisions, peculiarities and specific features of transnational crimes. As the cybercrime can be considered as the type of transnational crime, the provisions of the followed convention has to be mention too.

**The Convention on Cybercrime** (Budapest Convention on Cybercrime, the Budapest Convention) is the first international treaty seeking to address computer crime and Internet crimes by harmonizing national laws, improving investigative techniques and increasing cooperation among nations. It was drawn up by the Council of Europe in Strasbourgh with the active participation of the Council of Europe’s observer states Canada, Japan and China.

The Convention and its Explanatory Report was adopted by the Committee of Ministers of the Council of Europe at its 109th Session on 8 November 2001. It was opened for signature in Budapest, on 23 November 2001 and it entered into force on 1 July 2004. As of 22 October 2012, 37 states had signed, ratified and acceded to the convention; while a further 10 states had signed the convention but not ratified it.

On 1 March 2006 the Additional Protocol to the Convention on Cybercrime came into force. Those states that have ratified the additional protocol are requited to criminalize the dissemination of racist and xenophobic material through computer systems, as well as of racist and xenophobic-motivated threats and insults.

The Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography, hate crimes and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and lawful interception. Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation.

The Convention aims principally at:

1. Harmonizing the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime;

2. 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;

3) Setting up a fast and effective regime of international co-operation.

The following offences are defined by the Convention: illegal access, illegal interception, data interference, and system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography and offences related to copyright and neighboring rights.

It also 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. In addition, the Convention contains a provision on a specific type of transborder access to stored computer data which does not require mutual assistance (with consent or where publicly available) and provides for the setting up of a 24/7 network for ensuring speedy assistance among the signatory parties.

Cybercrime is considered as one of the grates challenges of humanity today that is why it is obvious needed to be researched. More and more articles, scientific studies, books, researches and theoretical manuals appear each year which is one of the key steps to fight the problem.

Мансуро

МЕЖДУНАРОДНО-ПРАВОВОЕ ПРОТИВОДЕЙСТВИЕ ТРАНСНАЦИОНАЛЬНОЙ НАРКОПРЕСТУПНОСТИ

Рост наркотизации населения существенно сказывается на росте преступности в целом. Увеличивается не только число преступлений, связанных с незаконным оборотом наркотиков, но и количество корыстно-насильственных посягательств, совершаемых наркоманами в целях получения средств для приобретения наркотиков. По данным Всемирного Доклада ОНН о наркотиках 2010 г. численность людей, употребляющих наркотики, в мире оценивает-
Палєєва Ю. С.
ПОГЛЯД НА ІНСТИТУТ ЕКСТРАДИЦІЇ В КОНТЕКСТІ ОСТАННИХ ЗМІН НАЦІОНАЛЬНОГО ЗАКОНОДАВСТВА УКРАЇНИ .............................................. 374

Бдоян А. А.
ВЛЯННЯ НОРМ МІЖДУНАРОДНОГО ПРАВА НА УГОЛОВНО-
ІСПОЛНИТЕЛЬНУ ПОЛІТИКУ РОССІЇ В ОТНОШЕНІЙ ПРИМЕНЕНІЯ
НАКАЗАНІЙ НЕ СВЯЗАННИХ С ЛИШЕНІЕМ СВОБОДИ ......................... 377

Бирёв Д. В.
МІЖДУНАРОДНОЕ ПРАВО И СОВРЕМЕННЫЕ МЕХАНИЗМЫ
ПРОТИВОДЕЙСТВИЯ ТЕРРОРИЗМУ .................................................... 381

Прачук М. П.
ПРАВОВЕ РЕГУЛЬЮВАННЯ МІЖНАРОДНОГО ТЕРРОРИЗМУ:
ПРОБЛЕМИ ТА ПЕРСПЕКТИВИ ......................................................... 383

Gayday К. М.
UNIVERSAL JURISDICTION IN ABSENTIA: MEANINGLESS OR REASONABLE
DISTINCTION? .......................................................................................... 387

Гнатенко С. С.
СПІВВІДНОШЕННЯ КРИМІНАЛЬНОГО ПРАВА УКРАЇНИ И МІЖНАРОДНОГО
КРИМІНАЛЬНОГО ПРАВА. ПРОЦЕС ГАРМОНІЗАЦІЇ ТА АДАПТАЦІЇ ........ 391

Колоколов А. Е.
ПРОБЛЕМЫ ОПРЕДЕЛЕНИЯ ПОНЯТИЯ «ТЕРРОРИЗМ» И ИХ ПОСЛЕДСТВИЯ . 393

Кравченко Ю. О.
ПРАВОВА ОСНОВА МИРОТВОРЧОЇ ДІЯЛЬНОСТІ:
ПРОБЛЕМАТИКА ТА ПЕРСПЕКТИВИ РОЗВИТКУ ................................... 397

Куртинець М. І.
«ГЕНОЦИД»: ІСТОРІЯ СТВОРЕННЯ ТА УТВЕРДЖЕННЯ
У МІЖНАРОДНОМУ ПРАВІ ................................................................. 402

Kuzmin E. E.
THE TRANSNATIONAL DIMENSION OF CYBERCRIME ......................... 405

Мансуров Т. И.
МІЖДУНАРОДНО-ПРАВОВЕ ПРОТИВОДЕЙСТВИЕ
ТРАНСНАЦІОНАЛЬНОЙ НАРКОПРЕСТУПНОСТІ. ............................. 409

Мелихов И. Ю.
СООТВЕТСТВИЕ ПОЛОЖЕНИЯ В РОССИЙСКОЙ ПЕНИТЕНЦИАРНОЙ
СИСТЕМЕ ТРЕБОВАНИЯМ МІЖДУНАРОДНЫХ СТАНДАРТОВ ПО ВОПРОСУ
ПРАВОВОГО СТАТУСА ПЕРСОНАЛА .................................................... 413

Пісов М. П.
НАЙМАНСТВО СУТНІСТЬ, НОВІТНІ ТЕНДЕНЦІЇ РОЗВИТКУ
ТА ПРОБЛЕМИ ПРОТИДІ ................................................................. 417

Попова Т. А.
КОНТРОЛЬ ДЕЯТЕЛЬНОСТИ ПЕНИТЕНЦІАРНОЇ СИСТЕМИ:
МІЖДУНАРОДНО-ПРАВОВЕ ОСНОВЫ И РОССИЙСКИЙ ОПЫТ
РЕАЛИЗАЦИИ ............................................................................................ 421

Шинкарук Т. Р.
ЗАСОБИ ПРОТИДІ ТОРГІВЛІ ЛЮДЬМИ: МІЖНАРОДНО-ПРАВОВИЙ ДОСВІД 425
Наукове видання

МІЖНАРОДНІ ЧИТАННЯ
з міжнародного права
пам'яті професора
П.Є. КАЗАНСЬКОГО

Матеріали
третьої міжнародної наукової конференції

Одеса, Україна
2-3 листопада 2012