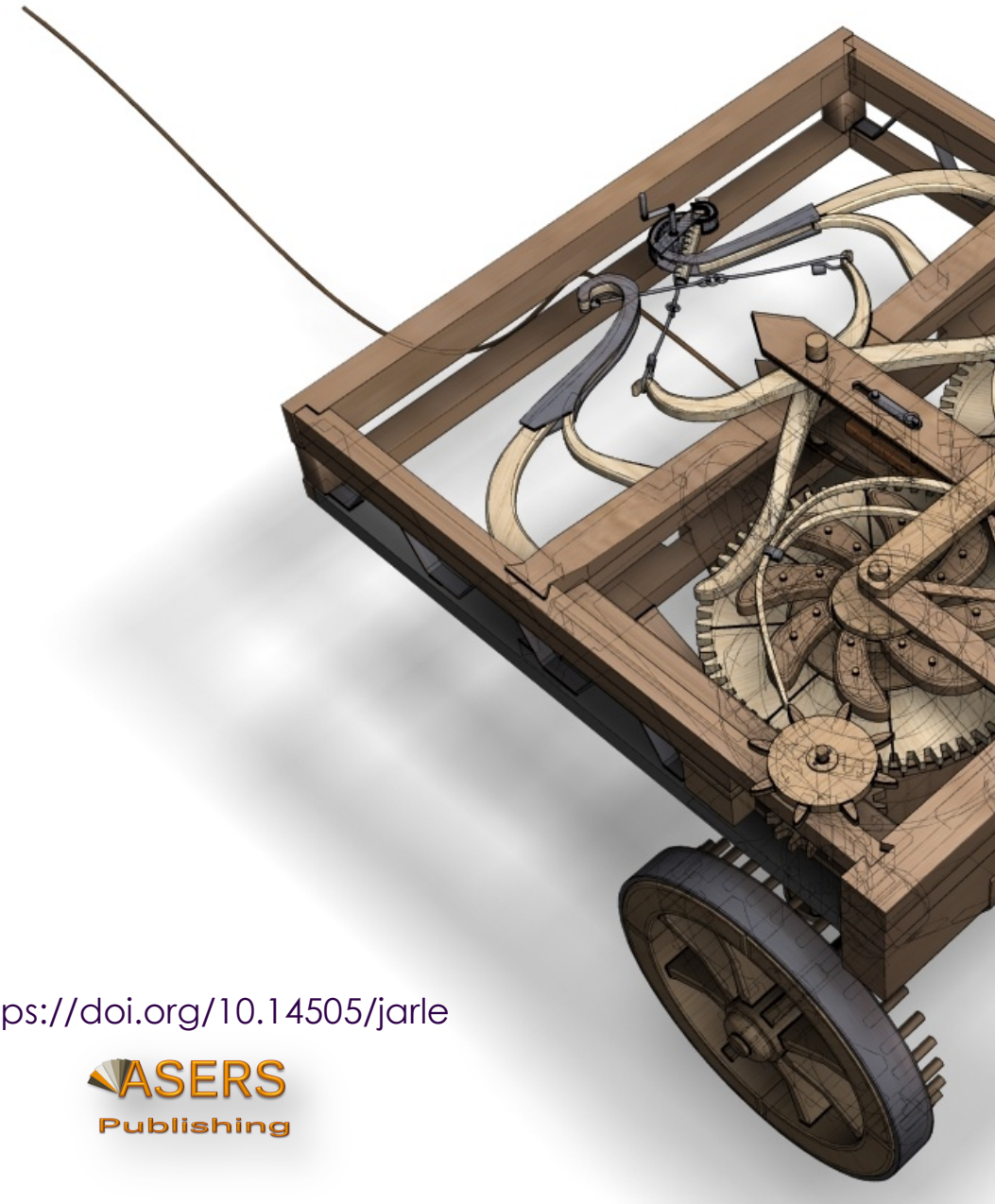
ASERS

Journal of Advanced Research in Law and Economics



Quarterly

Volume VIII
Issue 3(25)
Summer 2017

ISSN: 2068-696X
Journal's DOI: https://doi.org/10.14505/jarle

ASERS Publishing

Summer 2017
Volume VIII, Issue 3(25)

Editor in Chief
Madalina Constantinescu
Association for Sustainable Education Research and Science, and *Spiru Haret* University, **Romania**

Co-Editors

Russell Pittman
International Technical Assistance Economic Analysis Group Antitrust Division, **USA**

Eric Langlais
EconomiX CNRS and Université Paris Ouest-Nanterre, **France**

Editorial Advisory Board

Huseyin Arasli
Eastern Mediterranean University, **North Cyprus**

Jean-Paul Gaertner
Ecole de Management de Strasbourg, **France**

Shankar Gargh
Editor in Chief of Advanced in Management, **India**

Arvi Kuura
Pärnu College, University of Tartu, **Estonia**

Piotr Misztal
Technical University of Radom, Economic Department, **Poland**

Adrian Moise
Spiru Haret University, **Romania**

Peter Sturm
Université de Grenoble 1 Joseph Fourier, **France**

Rajesh K. Pillania
Management Developement Institute, **India**

Rachel Price-Kreitz
Ecole de Management de Strasbourg, **France**

Laura Ungureanu
Association for Sustainable Education Research and Science, Romania, **Romania**

Hans-Jürgen Weißbach, University of Applied Sciences - Frankfurt am Main, **Germany**

Contents:

1 **From Ideal to Reality: Constitutional Engineering of the XXI Century**
by Marianna Abramova, Anna Popova, Oxana Vasilieva, Marina Milovanova, and Nikolay Polishchuk ... 703

2 **Insurers' Responsibility in Insurance Liability**
by Natalia A. Antonova, and Elena N. Lunyova ... 708

3 **Childhood Legal Protection in Kazakhstan**
by Nurlan Apakhayev, Kultay Adilova, Dina Bugybay, Gulyiya Mukaldyeva, Gulzhan N. Mukhamadiyeva, and Bakhytkali M. Koshpenbetov ... 714

4 **Legal Basis for Ensuring Freedom of Access to Information on the Operation of State Administration Bodies in Kazakhstan**
by Nurlan Apakhayev, Kuanysh Koishybaiuly, Gulnura Khudaiberdina, Ainur Urisbayeva, Zhanna A. Khamzina, and Yermek A. Buribayev ... 722

5 **Topical Issues of Criminal Law and Lawsuit in Kazakhstan: Assignment of Punishment under Criminal Law**
by Aliya Baisseitova, Zhanar Kegembayeva, Irina Shalkarova (Kim), Omerbay Smailov, and Gulnar Sagynbekova ... 730

6 **Improvement of Legal Measures to Prevent Crime with Regard to Minors in Kazakhstan**
by Svetlana M. Baimoldina, and Sholpan A. Zabikh ... 738

7 **Agile Transformation of the Russian Sector of Economy According to the Legislative Framework**
by Elena S. Balashova, and Elizaveta A. Gromova ... 749

8 **Legal Regulation of Municipal Solid Waste Treatment in the Transition of Developing Countries to 'Green Economy'**
by Dauren Bekezhanov, and Lazzat Yerkinbayeva ... 754

9 **The Policy of Combating Crimes Related to Trafficking in Persons: Conceptual Apparatus and Structural Elements**
by Alimzhan Bekmagambetov ... 763

10 **Legal Support of Economic Mechanism of Groundwater Protection and Use Regulation in Central Asia Region**
by Alina Borodina, and Lazzat K. Yerkinbayeva ... 773

11 **Fairness in Dismissal for Business Reasons in Indonesia**
by Budi Santoso ... 783

12 **Uncertainty of the Legal Regulation of Relations in the Sphere of Comparative Advertising: the Essence of the Problem and Possible Solutions**
by Evgenia E. Frolova, Ksenia M. Belikova, Natalia V. Badaeva, and Irina V. Ermakova ... 792

Summer 2017
Volume VIII, Issue 3(25)

13 **The Concept of Real Right in India and South Africa: Specifics of National Regulation and Trends of Harmonization of Law**

by Evgenia Frolova, Ksenia Belikova, Natalia Badaeva, Irina Belozerova, and Victor Ulianischev ... 799

14 **Improvement Directions for the Mechanisms of Corruption Counteracting in Russian Uniform Information System of Procurement**

by Anton N. Gazetov ... 813

15 **Certain Problems of Fighting Ecocide**

by Oksana Y. Grechenkova ... 821

16 **Problems of Legal Regulation Improvement in the Sphere of Science, Technology and Innovation in Post-Soviet space in Keeping with Modern International Regulatory Trends**

by Oleg V. Gutnikov, Anna S. Dupan, and Vladimir P. Emelyantsev ... 821

17 **Syndicated Lending: Intensification of Transactions and Development of Legal Regulation in Modern Russia**

by Agnessa O. Inshakova, Alexander I. Goncharov, Olesya P. Kazachenok, and Svetlana Y. Kochetkova ... 838

18 **Institutional Aspects of Integration in the EEU: Problems and Prospects**

by Natalja Jemeljanova, Vladimir Kartashkin, Olga Meshcheryakova, and Anait Smbatyan ... 843

19 **Problems of Fighting Crimes on the Internet**

by Elena Anatolyevna Kirillova, Rashad Afatovich Kurbanov, Natalia Viktorovna Svechnikova, Teymur El'darovich Zul'fugarzade, and Sergey Sergeevich Zenin ... 849

20 **Occurrence of Resolutive Condition of a Deed as a Juridical Fact in Civil Law of Ukraine**

by Anatoliy V. Kostruba ... 857

21 **The Place and Role of Professional Legal Consciousness in Various Legal Activities**

by Vita Volodymyrivna Kovalska ... 865

22 **Legal Defense of Interethnic and Religious Relationships: Russian and International Experience**

by Elena Kunts, and Vladimir Golubovskii ... 871

23 **Social Foundation and Sociological Substantiation of Positive Legal Responsibility**

by Dmitry A. Lipinsky, and Tatiana N. Ivanova ... 878

ASERS Publishing
Copyright © 2017, by ASERS® Publishing.
All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except under the terms of the Romanian Copyright, Designs and Patents Law, without the permission in writing of the Publisher.

Requests to the Publisher should be addressed to the Permissions Department of ASERS Publishing: asers@asers.eu and apg@aserspublishing.eu

http://journals.aserspublishing.eu
ISSN 2068-696X
Journal DOI: https://doi.org/10.14505/jarle
Journal's Issue DOI:
https://doi.org/10.14505/jarle.v8.3(25).00

Summer 2017
Volume VIII, Issue 3(25)

24 **Concept and Model of Local Self-Government Using Organizational Design and Public Communications**
by Marina N. Lukiyanova, Elena F. Nikitskaya, and Nadezhda V. Sedova ... 887

25 **Challenges of Court Orders Enforcement**
by Maksim Mateikovich ... 899

26 **Escrow: International Experience and Perspectives of Application in Russia**
by Evgenia V. Medentseva, and Maksim A. Tokmakov ... 906

27 **Police of the Stavropol Province of the Russian Empire in the Second Half of the XIX Century**
Lyudmila V. Medveditskova, Julia A. Burlova, Rashid A. Atayev, Andrey N. Osyak, Viktor V. Shanko, and Anatoly K. Kiselev ... 910

28 **Legal Ideology as an Element of the Relationship of Civil Society and the State**
Viktor Yu. Melnikov, Yuri A. Kolesnikov, Alla V. Kiseleva, and Bika B. Dzhamalova ... 919

29 **Analogy in the Mechanism of Judicial Control over the 'Golden Parachutes' Amount**
by Viktor A. Mikryukov ... 926

30 **Analysis of Illegal Interception of a Computer Data Transmission Crime in Romanian Legislation**
by Adrian Cristian Moise ... 933

31 **The Modern Understanding of Franchising in Theory and Legislation**
by Aigul A. Nukusheva, Ulan M. Khamzin, Gulzhazira A. Ilyassova, Unzila Shapak, and Inkar T. Mussayeva ... 946

32 **Process Approach in Results-oriented Public Administration**
by Dulpariz Nurhalieva, Serik Omirbaev, Bazhan Turebekova, and Zhamila Bopiyeva ... 950

33 **Legal Framework for Combating Corruption in Nigeria -The Upstream Petroleum Sector in Perspective**
by Olusola Joshua Olujobi ... 956

ASERS Publishing
Copyright © 2017, by ASERS® Publishing.
All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except under the terms of the Romanian Copyright, Designs and Patents Law, without the permission in writing of the Publisher.

Requests to the Publisher should be addressed to the Permissions Department of ASERS Publishing: asers@asers.eu and apg@aserspublishing.eu

http://journals.aserspublishing.eu
ISSN 2068-696X
Journal DOI: https://doi.org/10.14505/jarle
Journal's Issue DOI:
https://doi.org/10.14505/jarle.v8.3(25).00

Summer 2017
Volume VIII, Issue 3(25)

34 **Status of Refugees in Accordance with the International Law and Legislation of Kazakhstan**

by Ayman B. Omarova, Nurlan Apakhayev, Kuanysh Koishybaiuly, Tleubek Tleuov, Yermek A. Buribayev, and Zhanna A. Khamzina ... 971

35 **On the National Security Correlation with Freedom of Speech in Kazakhstan**

by Yesbol Omirzhanov, Zulfiya Baimagambetova, Almagul Tusupova, Roza Omirtay, and Serik Uteuliev ... 980

36 **On the Question of the Concept and Forms of Cyberbullying in Russia**

by Nikolai Ivanovich Polishchuk, Sergei Mikhailovich Vorobyov, Alexandra Andreevna Orlova, and Edgar Parhamovich Abovyan ... 987

37 **The Experience of the European Union in the Field of Administrative and Legal Support for Asset-Grabbing Prevention**

by Roman Volodymyrovych Shapoval, Olga Ivanivna Demenko, and Khrystyna Volodymyrivna Solntseva ... 994

38 **Modern Paradigms of Legal Consciousness and Development of Legal Awareness in Post-Socialist Space**

by Galina V. Stankevich, Maxim I. Tsapko, Ruzanna A. Babayan, Radmila E. Arutyunian, and Polina N. Durneva ... 1009

39 **Rechssttaat and Rule of Law: Some Aspects**

by Zhalgas Temirbekov, Alpysbay Zhussupov, Aliya Orazbayeva, Dina Suleimenova, and Raushan Omarova ... 1017

ASERS Publishing
Copyright © 2017, by ASERS® Publishing.
All rights reserved.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except under the terms of the Romanian Copyright, Designs and Patents Law, without the permission in writing of the Publisher.

Requests to the Publisher should be addressed to the Permissions Department of ASERS Publishing: asers@asers.eu and apg@aserspublishing.eu

http://journals.aserspublishing.eu
ISSN 2068-696X
Journal DOI: https://doi.org/10.14505/jarle
Journal's Issue DOI:
https://doi.org/10.14505/jarle.v8.3(25).00

Call for Papers
Volume VIII, Issue 5(27), Fall 2017

Journal of Advanced Research in Law and Economics

Journal of Advanced Research in Law and Economics is designed to provide an outlet for theoretical and empirical research on the interface between economics and law. The Journal explores the various understandings that economic approaches shed on legal institutions.

Journal of Advanced Research in Law and Economics publishes theoretical and empirical peer–reviewed research in law and economics–related subjects. Referees are chosen with one criterion in mind: simultaneously, one should be a lawyer and the other an economist. The journal is edited for readability both lawyers and economists scholars and specialized practitioners count among its readers.

To explore the various understandings that economic approaches shed on legal institutions, the Review applies to legal issues the insights developed in economic disciplines such as microeconomics and game theory, finance, econometrics, and decision theory, as well as in related disciplines such as political economy and public choice, behavioral economics and social psychology. Also, *Journal of Advanced Research in Law and Economics* publishes research on a broad range of topics including the economic analysis of regulation and the behavior of regulated firms, the political economy of legislation and legislative processes, law and finance, corporate finance and governance, and industrial organization.

Its approach is broad–ranging with respect both to methodology and to subject matter. It embraces interrelationships between economics and procedural or substantive law (including international and European Community law) and also legal institutions, jurisprudence, and legal and politico – legal theory.

The quarterly journal reaches an international community of scholars in law and economics.

Submissions to *Journal of Advanced Research in Law and Economics* are welcome. The paper must be an original unpublished work written in English (consistent British or American), not under consideration by other journals.

Journal of Advanced Research in Law and Economics is currently indexed in SCOPUS, EconLit, RePec, CEEOL, EBSCO, ProQuest, and Cabell's Directory.

Invited manuscripts will be due till July 1st, 2017, and shall go through the usual, albeit somewhat expedited, refereeing process.

Deadline for submission of proposals:	1st of July 2017
Expected Publication Date:	September 2017
Web:	http://journals.aserspublishing.eu
E–mail:	jarle@aserspublishing.eu

Full author's guidelines are available from: http://journals.aserspublishing.eu/jarle/about

DOI: https://doi.org/10.14505/jarle.v8.3(25).19

Problems of Fighting Crimes on the Internet

Elena Anatolyevna KIRILLOVA
Southwest State University, Kursk, Russia
debryansk@mail.ru

Rashad Afatovich KURBANOV
Plekhanov Russian University of Economics, Moscow, Russia
Kurbanov.RA@rea.ru.

Natalia Viktorovna SVECHNIKOVA
Plekhanov Russian University of Economics, Moscow, Russia
Svetchnikova.NV@rea.ru

Teymur El'darovich ZUL'FUGARZADE
Plekhanov Russian University of Economics, Moscow, Russia
teymurz@yandex.ru

Sergey Sergeevich ZENIN
Kutafin Moscow State Law University, Russian Penitentiary Service Research Institute, Moscow, Russia
zeninsergei@mail.ru

Suggested Citation:

Kirillova, E.A. *et al.* 2017. Problems of Fighting Crimes on the Internet. *Journal of Advanced Research in Law and Economics*, Volume VIII, Summer, 3(25): 849 – 856. DOI: 10.14505/jarle.v8.3(25).19. Available from: http://journals.aserspublishing.eu/jarle/index

Article's History:

Received March, 2017; *Revised* April, 2017; *Published* June, 2017.
Copyright © 2017, by ASERS® Publishing. All rights reserved.

Abstract:

This article considers the problems of fighting crimes on the Internet, and defines new criminal acts committed by means of global computer networks. The aim of the study is to develop a categorical conceptual instrument, to separate a new type of cybercrime. The methodological basis of the study was the dialectic, comparative legal, sociological, systemic-structural and statistical methods as well as case study method – the method of active problem-situation analysis, by means of which the identification, selection and problem-solving in order to combat cybercrime was performed. The conducted study allows to offer the authors' definition of cyberterrorism and to identify the distinctive features of cyberterrorism, to allocate it in an independent kind of a crime and offer to include it in the Convention on Cybercrime as a separate article.

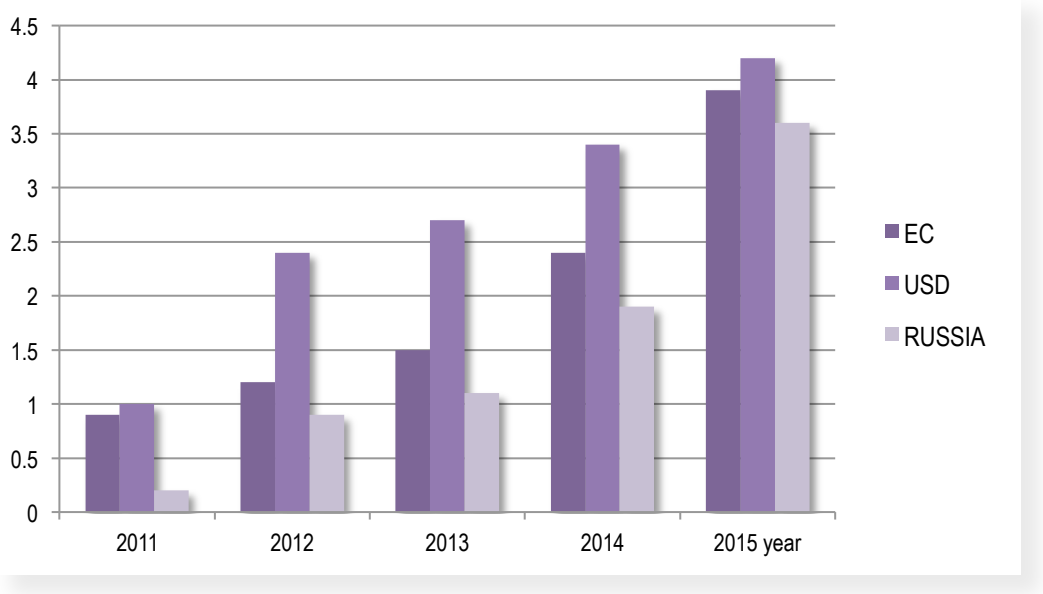
Keywords: cybercrime; information technology; terrorism; Internet

JEL classification: K24; K10; P37.

Introduction

With the increasing use of information technologies in various spheres of human activity, their use in committing crimes also grows. The member countries of the EU are among the world leaders in terms of Internet penetration. According to Internet World Stats, as of March 31, 2011, the total number of EU users is 338,420,555 people, the penetration rate is 67.3%, the increase in the number of users for the period of 2012-2015 amounted to 258,5%. In terms of the Internet penetration, EU countries are ahead of the European region as a whole (67.3% of the EU at 58.3% in Europe), and in the world second only to North America (78.3%). However, some EU members have penetration rates of the Internet far surpassing the United States and Canada (Figure 1).

Figure 1. Indicators of Internet penetration



In recent years, the use of the Internet creates more complex criminal processes. Against the rapid criminalization of social relations, the network crime is transforming (its growth, the increase in its organized nature, expanding the scope of criminal interests, the complication of the applied criminal schemes) as a natural world process, directly connected to a significant increase in the role of information and communication technologies in the information society (Brewster *et al.* 2015). The character of the criminological situation in the network today is set by representatives of organized crime (Berger *et al.* 2016).

The legislation and judicial practice do not always timely respond to these changes, resulting in legal gaps and violations of the legitimate rights and interests of citizens. Western researchers correctly believe that the law must adapt to new realities (Staniforth 2014).

The aim of the study is to define the concept of 'cyberterrorism', to highlight its characteristics and legal status.

The problem of crime on the Internet was considered by many scientists in their research. Levin and McDevitt (2015) investigated the features of cybercrime, Shipley and Bowker (2014) identified the methods of prevention of cybercrime; Furnell *et al.* (2015) revealed the essential features of crime in the Internet; Staniforth (2014) considered the practical aspects of cybercrime; Shipley and Bowker (2014) investigated the causes of crimes in the Internet; Solak and Topaloglu (2015) analyzed the crimes and their consequences in the Internet; Berger *et al.* (2016) paid special attention to DNS traffic when committing cybercrime; Al-Garadi *et al.* (2016) studied cybercrime at the present stage. It should be mentioned that most authors focused on the study of legal problems of the crimes, other types of socially dangerous acts, which thanks to information technology have reached new qualitative and quantitative levels; they did not raise or considered new types of cybercrimes. Today the world community does not have a common view on the legal issues of cybercrime in the global information and communication networks.

1. Method

The methodological basis of the research was the dialectic, comparative legal, sociological, systemic-structural and statistical methods, as well as the method of social experiment.

The comparative legal method includes the analysis of current legislation and judicial practice of foreign countries.

The use of concrete-sociological method allowed us to collect reliable information about the state of cybercrime, its quantitative and qualitative parameters, as well as about the peculiarities of practical application of existing legislation, including its problematic aspects.

During the social experiment, the construction of the most probable variants of development of the legal situations related to cybercrime was possible, as well as the search for an optimal solution of relevant problems.

In this study, we used the case study method – the method of active problem-situation analysis, with the help of which was carried out the following: the identification, selection and solution of problems in the fight against cybercrime; working with information – understanding the values of items described in the situation of offences in the Internet; analysis and synthesis of information and arguments with the aim to develop proposals to combat cybercrime; working with assumptions and conclusions; evaluation of alternatives and decision-making in law enforcement practice on improving it.

2. Results

The national infrastructure of any modern state is closely connected with the use of the latest computer technology. Daily activities of banking and energy systems, air traffic control, transportation network, even the ambulance services are totally dependent on reliable and safe operation of the automated computing systems. From year to year, the number of cyber-attacks on the websites of infrastructure and defense companies is rapidly increasing (Solak and Topaloglu 2015).

Today, many researchers consider the Islamic State of Iraq and the Levant (ISIL) to be the most dangerous group (Al-Garadi *et al.* 2016). In November 2015, American researchers counted at least 60 terrorist groups around the world who joined the global network of the Islamic State; many of them were previously associated with al-Qaeda (Levin and McDevitt 2015)). At the end of 2015, the group established an information center al-Hayat, broadcasting in English, German, Russian and French. The English-language online magazine 'Dabic' is spread on the Internet, and the strategy of ISIL in social media has been so effective that it even became the subject of research at the Brookings institution, USA (Goodman 2010). By analyzing the international experience, the judicial practice, we can highlight the most important legal issues of cybercrime at the present stage (Al-Garadi *et al.* 2016).

The basic problem of the fight against crime on the Internet is the transnationality of the network itself and the absence of monitoring mechanisms needed for enforcement. The lack of mechanisms for the control of the network from the inside, together with its accessibility and ease of use, become one of the major problems of global information community. The decentralized structure of the network and the lack of national borders in cyberspace led to growing opportunities for crime and delayed the development of legal control in the sphere of use of information networks in committing crimes for years (Frunza 2016).

In recent years, information networks are developing too quickly, so the existing control mechanisms have no time to react to new challenges. Cloud computing, automation of attacks, the vulnerability of personal information in social networks, the proliferation of so-called 'information weapons', for example the, viruses – this is an incomplete list of new security threats at the international level.

At that the crime does not require much effort and cost – it is enough to have a computer, software and connection to the information network. There are special forums where you can purchase the software for committing crimes, stolen credit card numbers and user credentials, and also use assistance services in committing electronic theft and attacks on computer systems (Furnell *et al.* 2015).

Researchers have identified another problem, which leads to difficulties in fighting cybercrime – it is the automation and speed of use of the Internet (Konradt *et al.* 2016). Computer data can be transmitted from one spot of the world to another in a few seconds; almost any data transmission in the network usually involves multiple countries, as information is broken into pieces and passes through the most convenient and available channels (Ibrahim 2016). It is very difficult to control the transmission of data in terms of their volume and number of users (Shipley and Bowker 2014). The offender, the victim, the server with the necessary information can be situated in different countries and on different continents; therefore, the cooperation of law enforcement agencies of several countries in cybercrime investigations is required. The automation increases the risk of committing multiple crimes without any financial and time costs (Frunza 2016).

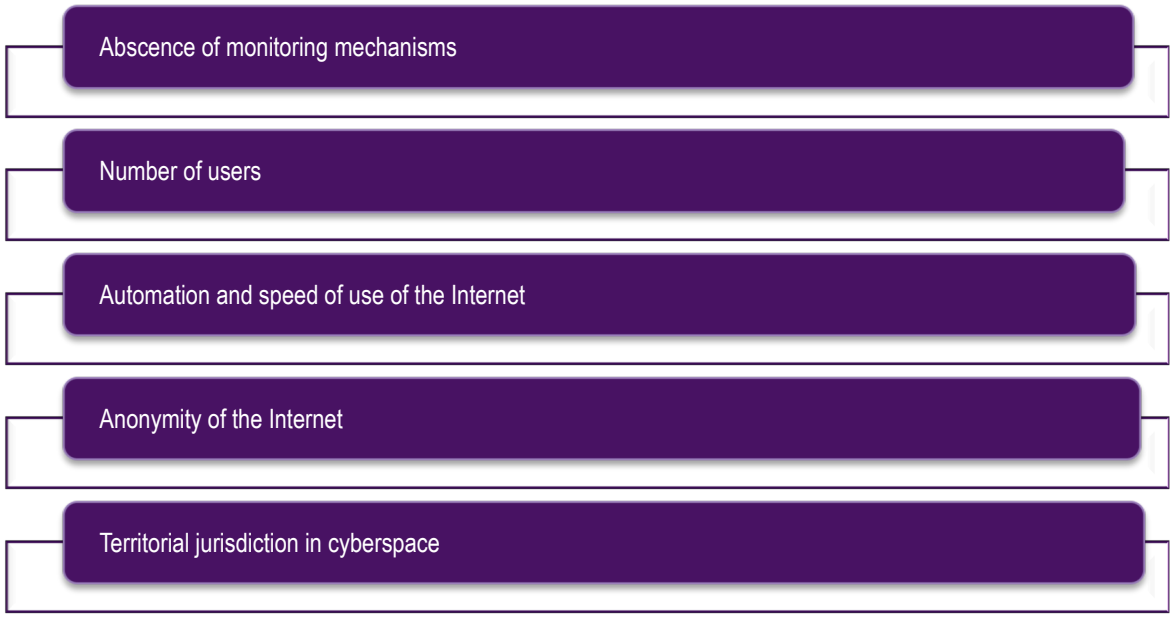
The anonymity of the Internet, the vulnerability of wireless access makes it difficult to locate criminals, as the crime can be used by a chain of servers (Katos and Bednar, 2008). The crimes can be committed through the Internet via a public access point such as Internet café; the technology allows to get illegal access to someone else's wireless network Wi-Fi. Thus, there is enough ways to hinder the investigation of crimes (Sammons and Cross 2017).

The existence of the problem of territorial jurisdiction in cyberspace and legal cooperation has been maintained by many researchers (Brewster *et al.* 2015). The investigation of crimes in information networks typically requires quick analysis and saving of computer data that is very vulnerable in nature and can quickly be destroyed. In this situation, traditional mechanisms of mutual legal assistance and the principle of sovereignty make the investigation of transnational cybercrimes problematic (DeTardo-Bora and Bora 2016). The

cooperation of law enforcement agencies requires compliance with many formalities. There is a question of the observance of the fundamental principle of nullum crimen, nulla poena sine lege, when the dual criminalization of the act is required: in the country, where the offender acted, and in the country where the victim is. The difference in criminalization of acts, the differences in the definition of the severity of the offence, complicate the process of law enforcement cooperation, sometimes making it impossible (Kirillova *et al.* 2014).

Thus, we can distinguish the following problems of fighting crimes on the Internet (Figure 2):

Figure 2. The main problems of the fight against cybercrime



In search of answers to the security challenges of the information society, the European Union has developed a three-stage approach covering:

(1) special measures in order to ensure network and information security;
(2) legal regulation of electronic communications, including issues of information protection and privacy;
(3) the fight against cybercrime.

Within the third specified direction, the EU developed and implemented a set of important initiatives, many of which are innovative in nature, the question of definitions is important.

The issue of classification of cybercrime causes the discussion among scientists (Jahankhani *et al.* 2014). The cyber crimes are divided into types depending on the object, the assault object, and the means of committing. For example, according to the assault object, there are the following types of cybercrime: offences against the confidentiality, integrity and availability of computer data and computer networks, economic computer crimes, computer crimes against personal rights and the inviolability of the private sphere, computer crimes against public and state interests (Konradt *et al.* 2016).

3. Discussion

In order to determine whether an act was a crime we need a sign of wrongfulness (criminalization), so the classification of cybercrime should be based on relevant legal acts, international treaties or national legislation. Taking into account that all countries – EU members are members of the Council of Europe, the European Union has gone the way of the adoption of its own acts in this sphere.

The most common classification is based on the norms of Convention on Cybercrime, adopted in the framework of the Council of Europe, according to which there are allocated five types of cybercrime:

(1) crimes against the confidentiality, integrity and availability of computer data and systems such as illegal access, illegal interception, data interference, interference in the system;
(2) crimes associated with the use of the computer as a means of committing crimes – namely, as a means of manipulation of the information. This group includes computer fraud and computer forgery;
(3) crimes associated with content (content data). The most common and punishable in almost all states of these cyber crimes are the crimes related to child pornography;

(4) offences related to infringement of copyright and related rights, at that the establishment of such offences is related by the document to the competence of national legislations of the states;
(5) the acts of racism and xenophobia committed through computer networks.

However, this Convention does not have a separate group for the use of the Internet for terrorist purposes, but this problem is being discussed. The lack of an agreed definition of terrorism at the international level currently hinders the debate on cyberterrorism as a phenomenon, the criminalization of which is necessary as a universal for the entire international community. States and international organizations are making efforts in order to combat Internet use by terrorist organizations – for example, at the European Union level, there is the Clean IT project, aimed at combating the phenomenon.

However, not only the European Union is exposed to cyber attacks; in recent years the computing system of the armed forces, large companies, government agencies of the United States are constantly attacked from cyberspace. For example, the computers of the Pentagon can be exposed to dozens of attacks per day. At that, of particular concern of the experts is organized attempt in this regard; the U.S. created a special presidential Commission, including well-known experts in the field of information technology. The Commission called the most vulnerable points in the infrastructure of the United States the energy, telecommunications, aviation dispatch systems, financial, electronic transmission, government information and military weapon control system (armament), and recommended the government to strengthen the protection of such objects (Willems 2011).

The concept of 'cyberterrorism' was founded by the merger of two words: 'cyber' ('cyberspace') and 'terrorism' (Gorge 2007). The terrorism, terrorists, terrorist activity – these concepts appear in the media almost daily, but up to now there is no universal definition. The problem of defining the terrorism exists since the manifestation of this phenomenon in public and political life. Thus, according to the American scientist Cassis, there are over one hundred definitions of terrorism (Cassese 2001).

The analysis of the existing approaches to the definition of terrorism shows that the majority of world scientists see the phenomenon as an expression of dissatisfaction with the existing socio-political situation that violates the legal foundations of life and is associated with ideological and psychological expression (Tropina 2010). Each of the researchers, according to their academic commitment, place the primary emphasis on one of these grounds (Authorities Losing the Battle against Cybercrime, Says UK's National Crime Agency 2016). So, terrorism as a particular form of violence is defined as conscious and purposeful use by anyone of the violence or threat of violence in order to force political leaders to implement political, economic, religious or ideological goals of terrorist organizations. In the field of international relations, terrorism is an acute threat to international security because it endangers the stability and peace in relations between individual states and groups of states, provokes the tensions between them, often fueled dangerous international conflicts, prevent their resolution (Kenney 2015). As rightly mentioned by many experts, the terrorism in the international arena acts as a tool of interference in the internal affairs of states, disrupts international relations, violates human rights, international law (Shipley and Bowker 2014). That's why the problem of terrorism is to be considered at the international level as a direct threat to international security and the threat of cyberterrorism – as a second component of such threats. Based on the primary concept of terrorism and its combination with the virtual space, we can derive the following definition. Cyberterrorism is a complex action, which is expressed in a deliberate, politically motivated attack on information, processed by computer and computer systems, endanger the life or health of people or the onset of other grave consequences, if such actions were the performed for the purpose of violating public security, intimidation of the population, provocation of the military conflict. One of the ways of cyber terrorism is a politically motivated attack on information. It is a direct management of society by means of preventive deterrence. This is manifested in the threat of violence, maintaining a state of constant fear with the purpose of achieving certain political or other goals, coercion to certain actions, drawing attention to the identity of a terrorist or cyberterrorist organizations, which it represents.

Based on the analysis of scientific literature, international documents and legislation of several countries, it seems to be possible to select some of the distinguishing features of cyber-terrorism as a legal phenomenon (Tehrani *et al.* 2013).

The first distinguishing characteristic of cyberterrorism is that it creates a common danger, which occurs as a result of the threat or commission of a socially dangerous actions. The danger must be real and threaten to the public.

The second distinctive characteristic of cyberterrorism is that the cyberterrorism acts have a public character and get public publicity. Today, cyber terrorism is indeed a form of violence aimed at the mass perception.

The third distinctive characteristic of cyberterrorism noted by the researchers is the deliberate creation of climate of tension, depression, fear on a social level, which is an objectively existing socio-psychological factor, influencing others and driving them to any action in the interests of the cyberterrorists or acceptance of their conditions.

The fourth distinctive characteristic of cyberterrorism is that when making cyberterrorists act, the dangerous violence applies to some individuals or organizations for the purposes of the psychological impact and inclination to a certain behavior of others.

The fifth characteristic of cyberterrorism is the distance from the place of direct terrorist act, the anonymity of the criminals, a small material costs (since it does not require weapons, explosives), and the fact that it is almost impossible to predict and trace cyberterrorists attacks in real time

Based on the works of researchers of cyber-terrorism (Goodman *et al.* 2007), as a phenomenon that threatens the national security of the state, we can identify the following trends:

(1) The steady increase of created by it public danger, which is reflected in the fact that the general level of extremism and terrorism throughout the world is constantly increasing. It should also be noted that the modern achievements of scientific and technological progress increase the likelihood of initially peaceful technology as a means of cyber-attacks, and such their use to the detriment is sometimes not even perceived by the creators of these technologies.
(2) The scale of impact on different social layers. This trend is manifested in the use of cyberterrorists of information and communication networks and systems through which occurs the impact on large numbers of people (*e.g.*, social networks), at weak censorship or the complete absence of any control by the state, and in a quick and relatively cheap dissemination of information.
(3) The transformation of cyber-terrorism in a long-term factor in the political process. This is due to the lack of major successes in countering it in the last decade and the creation of new prerequisites for its further dissemination (globalization, scientific and technological progress), the worsening in a number of countries of the numerous centers of the struggle for the revision of state borders, religious, ideological and political contradictions.
(4) Increasing the level of its organization, which includes the creation of a deployed infrastructure of terrorist activities on the Internet, the coordination of ideological and political positions, exchange of information, coordination of ongoing actions and attacks without outside interference from the intelligence services and law enforcement.
(5) The increasing of sophistication and inhumanity of cyberterrorist acts due to the fact that today cyberterrorists have a real opportunity to disrupt the normal functioning of critical facilities of the state (nuclear reactors, biological and chemical laboratories, etc.), which would lead to an incalculable number of victims.
(6) The improvement of the technical equipment of cyberterrorists. The cyberterrorism refers to the technological forms of terrorism. Unlike traditional, this kind of terrorism uses in the acts of terrorism the latest achievements of science and technology in the field of computer and information technology and radio electronics.
(7) The politicization of cyberterrorism, manifested in the desire of cyberterrorists to influence government decision-making in order to weaken law enforcement, stopping legislative initiatives through violent means (theft or destruction of information, blackmail, threats, damage to computers).

In terms of world-wide increasing of the processes of globalization and formation of information society, cyberterrorism can act as an independent factor able to threaten individual states and the international community as a whole.

Conclusion

The economic and scientific-technical policy of connection of a state to global open networks should provide the protection of national information networks from cyberterrorism. This study allows to highlight the characteristics of cyberterrorism:

(1) The danger arises as a result of committing of socially dangerous acts, threatening an indefinite circle of persons.
(2) The acts of cyberterrorism are public and get common publicity.
(3) The deliberate creation of a climate of tension and fear on a social level.
(4) The violence is used against some individuals or organizations for the purposes of the psychological impact and inclination to a certain behavior of others.

(5) The distance from the place of direct terrorist act, the anonymity of the criminals, small material costs (since it does not require weapons, explosives), and the fact that it is almost impossible to predict and trace cyberterrorists attacks in real time.

It is proposed to define the concept of cyberterrorism and confirm it in international legal instruments. The cyberterrorism is a complex action, which is expressed in a deliberate, politically motivated attack on information, processed by computer and computer systems, endanger the life or health of people or the onset of other grave consequences, if such actions were the performed for the purpose of violating public security, intimidation of the population, provocation of the military conflict.

It seems necessary to include in the Convention on cybercrime a separate category for such kind of crimes like cyberterrorism or the use of cyberspace for terrorist purposes.

The conducted research allows to offer the authors' definition of 'cyberterrorism' and to make a proposal on the allocation of this crime in a separate type. Further studies will be conducted for a more detailed definition of a measure of responsibility for the act, perhaps researchers will offer the direction of unification of international legal acts in the field of combating cyber terrorism.

References

[1] Al-Garadi, M.A., Varathan, K.D., and Ravana, S.D. 2016. Cybercrime Detection in Online Communications: The Experimental Case of Cyberbullying Detection in the Twitter Network. *Computers in Human Behavior,* 63: 433-443.

[2] Brewster, B., Kemp, B., Galehbakhtiari, S., and Akhgar, B. 2015. Cybercrime: Attack Motivations and Implications for Big Data and National Security. In B. Akhgar, G.B. Saathoff, H.R. Arabnia, R. Hill, A. Staniforth, & P.S. Bayerl (Eds.), *Application of Big Data for National Security*. Oxford: Butterworth-Heinemann, pp. 108-127.

[3] Berger, A., D'Alconzo, A., Gansterer, W.N., and Pescapé, A. 2016. Mining Agile DNS Traffic Using Graph Analysis for Cybercrime Detection. *Computer Networks,* 100: 28-44.

[4] Cassese, A. 2001. *International Law*. Oxford: Oxford University Press, pp. 150-151.

[5] DeTardo-Bora, K.A., and Bora, D.J. 2016. Cybercrimes: An Overview of Contemporary Challenges and Impending Threats. In J. Sammons (Ed.), *Digital Forensics*. Amsterdam: Elsevier, pp. 119-132.

[6] Frunza, M.-C. 2016. Cybercrime. In M.-C. Frunza, *Introduction to the Theories and Varieties of Modern Crime in Financial Markets*. Amsterdam: Elsevier, pp. 207-220.

[7] Furnell, S., Emm, D., and Papadaki, M. 2015. The Challenge of Measuring Cyber-Dependent Crimes. *Computer Fraud & Security,* 2015(10): 5-12.

[8] Goodman, M. 2010. International Dimensions of Cybercrime. In S. Ghosh, & E. Turrini (Eds.), *Cybercrimes: A Multidisciplinary Analysis.* Berlin, Heidelberg: Springer, pp. 77-79.

[9] Goodman, S.E., Kirk, J.C., and Kirk, M.H. 2007. Cyberspace as a Medium for Terrorists. *Technological Forecasting and Social Change,* 74(2): 193-210.

[10] Gorge, M. 2007. Cyberterrorism: Hype or Reality? *Computer Fraud & Security*, 2007(2): 9-12.

[11] Ibrahim, S. 2016. Social and Contextual Taxonomy of Cybercrime: Socioeconomic Theory of Nigerian Cybercriminals. *International Journal of Law, Crime and Justice,* 47*:* 44-57.

[12] Jahankhani, H., Al-Nemrat, A., and Hosseinian-Far, A. 2014. Cybercrime Classification and Characteristics. In B. Akhgar, A. Staniforth, & F. Bosco (Eds.), *Cyber Crime and Cyber Terrorism Investigator's Handbook*. Amsterdam: Elsevier, pp. 149-164.

[13] Katos, V., and Bednar, P.M. 2008. A Cyber-Crime Investigation Framework. *Computer Standards & Interfaces,* 30(4): 223-228.

[14] Konradt, C., Schilling, A., and Werners, B. 2016. Phishing: An Economic Analysis of Cybercrime Perpetrators. *Computers & Security,* 58: 39-46.

[15] Kenney, M. 2015. Cyber-Terrorism in a Post-Stuxnet World. *Orbis,* 59(1): 111-128.

[16] Kirillova, Y.A., Vasilyeva, M.V., and Krohina, Y.A. 2014. Legal Protection of Copyright Items Inheritance in the Internet by Means of a Creative Commons License. *Review of European Studies,* 6(4): 232-238.

[17] Levin, J., and McDevitt, J. 2015. Hate Crimes. In N.J. Smelser, & P.B. Baltes (Eds.), *International Encyclopedia of the Social & Behavioral Sciences* (2nd ed.). Amsterdam: Elsevier, pp. 540-545.

[18] Sammons, J., and Cross, M. 2017. Cybercrime. In J. Sammons, & M. Cross, *The Basics of Cyber Safety*. Amsterdam: Elsevier, pp. 87-116.

[19] Shipley, T.G., and Bowker, A. 2014. Covert Operations on the Internet. In T.G. Shipley, & A. Bowker, *Investigating Internet Crimes*. Amsterdam: Elsevier, pp. 233-252.

[20] Solak, D., and Topaloglu, M. 2015. The Perception Analysis of Cyber Crimes in View of Computer Science Students. *Procedia – Social and Behavioral Sciences,* 182: 590-595.

[21] Staniforth, A. 2014. Police Investigation Processes: Practical Tools and techniques for Tackling Cyber Crimes. In B. Akhgar, A. Staniforth, & F. Bosco (Eds.), *Cyber Crime and Cyber Terrorism Investigator's Handbook*. Amsterdam: Elsevier, pp. 31-42.

[22] Willems, E. 2011. Cyber-Terrorism in the Process Industry. *Computer Fraud & Security,* 2011(3): 16-19.

[23] Shipley, T.G., and Bowker, A. 2014. Internet Criminals. In T.G. Shipley, & A. Bowker, *Investigating Internet Crimes*. Amsterdam: Elsevier, pp. 21-39.

[24] Tehrani, P.M., Manap, N.A., and Taji, H. 2013. Cyber Terrorism Challenges: The Need for a Global Response to a Multi-Jurisdictional Crime. *Computer Law & Security Review,* 29(3): 207-215.

[25] Tropina, T. 2010. Cybercrime and Organized Crime. *Freedom from Fear Magazine, 7: 3*.

ASERS

ASERS Publishing

Web: www.aserspublishing.eu and www.asers.eu
URL: http://journals.aserspublishing.eu
E-mail: jarle@aserspublishing.eu
ISSN 2068-696X
Journal DOI https://doi.org/10.14505/jarle
Journal's Issue DOI https://doi.org/10.14505/jarle.v8.3(25).00