New Global Legal Frameworks/Treaty on Cybercrime

Analysis and Set of Proposal

Dr. Tatiana Tropina
EWI Cybercrime Legal Working Group
Freiburg, Germany

***Abstract*— One of the goals of the EWI Legal Working Group on Cybercrime is to develop a set of proposals for a new treaty to fight crimes in cyberspace. The Working Group has concluded that the following set of principles can be discussed for development of the proposal.**

***Index Terms*—Cybercrime, computer crime**

I. INTRODUCTION

Cyberspace is often referred to as the fifth common domain – after land, sea, air and outer space (Schjølberg, 2010: 11). However, this domain is merely in its infancy with regard to international customs, co-ordination and control. Nonetheless, the increased importance of Information and Communication Technologies (ICTs) in all facets of global commerce and society is thrusting the issue of tackling cybercrime into the realm of multi-disciplinary regulation. With its anonymity, easiness of use, and speed of communications, possibility to share information across borders and reach a big audience Internet becomes a key enabler both for legitimate users and for those who exploit all benefits of global information networks to commit crimes, including terrorists and organized crime groups [1].

Once a country is connected to a global information network, it becomes vulnerable to cybercriminals operating anywhere in cyberspace, but especially from "safe havens" – countries, that are not a part of growing global effort to tackle cybercrime. Therefore, a state cannot remain safe solely by implementing legislative and technical measures at the national level. Consequently, concerns over different aspects of cybercrime and cybersecurity, such as financial crime, money laundering, child pornography, growing use of the Internet by terrorist and organized crime groups, cyberwarfare are now international issues. The openness and transnational character of the cyberspace means that the measures to fight cybercrime only as good as their weakest link.

From the global perspective, the weakest link is the states with less developed cybercrime legislation. This issue is often linked to the developing countries, where network deployment goes faster than the development of cybersecurity culture [2]. Cybercrime and cybersecurity is not only a problem for industrialized states that rely heavily on ICT infrastructure and services. A common misconception that developing countries have too many basic "bread and butter" problems [3] to solve (e.g., food, water, literacy, fighting traditional crime, poverty reduction, HIV, etc.), and thus the implementation of cybercrime legislation is not and shall not be one of the highest priorities for them. However, the lack of appropriate regulation in the area of fighting cybercrime can open a new gap between developed and developing countries (often referred as "the cybersecurity divide"). This potential gap can worsen the digital divide, undermine other efforts put in place to facilitate economic and social development, and, as a result, open a new schism "between (the) haves and have nots" [4]. Moreover, these countries may become the weakest link and the safe havens for cybercriminals attacking users in other states without a risk of being prosecuted.

Thus, the problem of tackling cybercrime can be solved only on the global level. In this regard, development of the international standards for harmonisation of national legal frameworks is a vital element infighting cybercrime. However, ten years after the most important instrument to fight cybercrime - Council of Europe Convention on Cybercrime was opened for signature, the international community still faces a number of challenges in reaching consensus on global legal solutions to address crimes in global information networks [5].

It has already become obvious that, in some areas, consensus is very hard to achieve: for example, the controversially debated Article 32b of the Convention on Cybercrime deterred some jurisdictions from joining the treaty. Some issues that have been widely discussed in recent years, like cyberterrorism or cyberwarfare, are still very sensitive: depending on the legal and cultural backgrounds, approaches to the legal solutions may vary significantly. Moreover, there is still no agreed definition of "terrorism" at an international

level, and approaches to this term may differ even within one country, let alone among different jurisdictions [6].

At the same time, existing standards in the area of cybercrime legislation need to be adapted to the new developments in information technology and cybercrime that have emerged over the last decade: cloud computing, identity theft, social networking crimes and scams, to name but a few.

A new approach to the international standards to fight cybercrime shall adequately balance the abovementioned challenges. Instead of creating unnecessary competition to the accepted rules, the goal is to supplement existing standards and develop them by covering new threats. Thus, on the one hand, the new standards shall take into account those legal tools that have been recognised. On the other hand, the development of the set of principles to fight cybercrime shall revise the drawbacks of existing approaches, including controversial issues such as Article32b of COE Convention or cyberterrorism, and avoid conflicts between national jurisdictions.

II. SET OF STANDARDS

One of the goals of the EWI Legal Working Group on Cybercrime is to develop a set of proposals for a new treaty to fight crimes in cyberspace. The Working Group has concluded that the following set of principles can be discussed for development of the proposal.

1) SUBSTANTIVE CRIMINAL LAW

A set of proper and sufficient definitions shall be agreed in a way compatible with the existing international approaches for the following:

- "Computer"
- "Computer system"
- "Computer data"
- "Content data"
- "Traffic data"
- "Service provider"

The set of standards shall include provisions covering the most common forms of cybercrime in a way compatible with the internationally recognised approaches:

- Illegal access to a computer system
- Illegal interception of non-public transmissions
- Data interference
- System interference
- Misuse of devices
- Computer-related forgery
- Computer-related fraud
- Offences related to child pornography
- SPAM
- Identity theft

A proposal for criminalisation of CIA offences shall not modify the existing approaches that are widely accepted and implemented by many states in order to avoid unnecessary competition.

The minimal set of standards shall not include controversial issues:

- Cyberterrorism
- Cyberwar and Cyberwarfare. To criminalise massive attacks against critical infrastructures, aggravated circumstances or qualified data/systems interference provision can be developed.

2) PROCEDURAL INSTRUMENTS

- The proposed treaty shall include the existing procedural instruments that are already applied by many states:
- Expedited preservation of stored computer data
- Expedited preservation and partial disclosure of traffic data
- Production order
- Provisions on search and seizure instruments
- Lawful collection of traffic data
- Lawful interception of content data

A treaty may include as an option the following provisions with the possibility for reservation:

- Registration obligation
- Use of remote forensic software and sophisticated technical instruments with the possibility to limit them only to the certain types of serious crimes.
- A set of procedural instruments shall be developed in compliance with the internationally recognised fundamental rights of the suspects.

3) JURISDICTION AND INTERNATIONAL CO-OPERATION

A treaty shall develop existing regulations on jurisdiction, providing the set of criteria that will enable the establishment of a sufficient link to claim the jurisdiction for cyber-offences, such as: the location of data, the existence of any effect in the prosecuting country; the existence of certain effects in the prosecuting country; the intention of the perpetrator to affect a certain country.

The standards for international co-operation should reflect international approaches to mutual legal assistance in fighting cybercrime.

A treaty shall include provisions on the creation of a designated 24/7 point of contact for requests.

A treaty shall not include controversial provisions such as provisions on trans-border searches (Article 32b of Council of Europe Convention on Cybercrime).

III. DRAFT OF THE TREATY: SUBSTANTIVE CRIMINAL LAW AND PROCEDURAL INSTRUMENTS

Taking into account existing legal instruments and approaches, the working group suggests the following preliminary draft for a global treaty, which have to be discussed with different stakeholders. The draft was developed with taking onto account the existing international approaches, such as Council of Europe Convention on Cybercrime, Commonwealth Model Law on Cybercrime and HIPCAR Model Legislative Text on Cybercrime.

Section 1. PRELIMINARY

Article 1. Statement of purpose

The purpose of this Treaty is to promote cooperation to prevent and combat cybercrime more effectively.

Article 2. Use of terms

For the purposes of this Treaty:

(a) "Computer system" shall mean a device or a group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of data or any other function;

(b) "Computer data" shall mean any representation of facts, concepts, information, machine-readable code or instructions, in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

(c) "Critical infrastructure" shall mean computer systems, devices, networks, computer programs, computer data, so vital to the state that the incapacity or destruction of or interference with such systems and assets would have a debilitating impact on security, national or economic security, national public health and safety, or any combination of those matters;

(d) "Traffic data" shall mean computer data that relates to a communication by means of a computer system, is generated by a computer system that is part of the chain of communication and indicates the communication's origin, destination, route, time date, size, duration or the type of underlying services.

(e) "Service provider" shall mean

i. any natural or legal person that provides to users of its service the ability to communicate by means of a computer system, and

ii. any other person that processes or stores computer data on behalf of such communication service or users of such service.

Section II. SUBSTANTIVE CRIMINAL LAW

Article 3. Illegal access to a computer system

Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences, when committed intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, access to the whole or any part of a computer system.

A State Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 4. Illegal interception of non-public transmissions

Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification, the interception made by technical means, of any non-public transmission to, from or within a computer system; or electromagnetic emissions from a computer system carrying such computer data.

A State Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system, or by circumventing protection measures implemented to prevent access to the content of non-public transmission.

Article 5. Data interference

Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification the damaging, deletion, deterioration, alteration of computer data, rendering computer data meaningless, useless or ineffective, obstruction, interruption or interference with the lawful use of computer data; or denial of access to computer data to any person authorized to access it.

A State Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 6. System interference

Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification the serious hindering or interfering of the functioning of a computer system or with a person who is lawfully using or operating a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification the serious hindering with a computer system that is exclusively for the use of critical infrastructure operations, or in the case in which such is not exclusively for the use of critical infrastructure operations, but it is used in critical infrastructure operations and such conduct affects that use or impacts the operations of critical infrastructure.

Article 7. Misuse of devices

Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification

the production, sale, procurement for use, import, distribution or otherwise making available of:

i. a device, including a computer program, that is designed or adapted for the purpose of committing an offence defined by the Articles 3-6 of this Treaty; or

ii. a computer password, access code or similar data by which the whole or any part of a computer system is capable of being accessed;

with the intent that it be used by any person for the purpose of committing an offence defined by the Articles 3-6 of this Treaty; or

possession of the item mentioned in subparagraph (a) (i) or (ii) with the intent that it be used by any person for the purpose of committing an offence defined by the Articles 3-6 of this Treaty. A State Party may require by law that a number of such items be possessed before criminal liability attaches.

This Article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 is not for the purpose of committing an offence established in accordance with Articles 3-6 of this Treaty, such as for the authorized testing or protection of a computer system.

A State Party may reserve the right not to apply paragraph 1 of this Article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 (a) (ii).

Article 8. Computer-related forgery

Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible.

A State Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article 9. Computer-related fraud

Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification the causing of a loss of property to another by:

a. any input, alteration, deletion or suppression of computer data,

b. any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

Article 10. Offences related to child pornography

Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, without lawful excuse or justification:

a. producing child pornography for the purpose of its distribution through a computer system;

b. offering or making available child pornography through a computer system;

c. distributing or transmitting child pornography through a computer system;

d. procuring child pornography through a computer system for oneself or for another person;

e. possessing child pornography in a computer system or on a computer-data storage medium.

f. knowingly obtains access, through information and communication technologies, to child pornography,

For the purpose of paragraph 1 above "child pornography" shall include pornographic material that visually depicts:

a. a minor engaged in sexually explicit conduct;

b. a person appearing to be a minor engaged in sexually explicit conduct;

c. realistic images representing a minor engaged in sexually explicit conduct.

For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A State Party may require a lower age-limit, which shall be not less than 16 years.

Each State Party may reserve the right not to apply, in whole or in part, paragraph 1(d), 1 (e) and 1(f), and 2(b), 2(c).

Article 11. SPAM

Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, without lawful excuse or justification:

Intentional initiation of the transmission of multiple electronic mail messages from or through such computer system; or

use of protected computer system to relay or retransmit multiple electronic mail messages, with the intent to deceive or mislead users, or any electronic mail or Internet service provider, as to the origin of such messages, or

c. material falsification of the header information in multiple electronic mail messages and intentional initiation of the transmission of such messages,

Each State Party may reserve the right not to apply, in whole or in part, paragraph 1.

Article 12. Identity theft

Each State Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification by using a computer system in any stage of the offence intentional transfer, possession, or use, without lawful excuse or justification, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a crime.

Section III. PROCEDURAL INSTRUMENTS

Article 13. Expedited preservation of stored computer data

Each State Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data that is reasonably required for the purposes of a criminal investigation is particularly vulnerable to loss or modification.

Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person’s possession or control, the State Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of 90 days, to enable the competent authorities to seek its disclosure. A State Party may provide for such an order to be subsequently renewed.

Each State Party shall adopt such legislative or other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.

The powers and procedures referred to in this article shall be subject to Articles 20 and 21.

Article 14. Expedited preservation and partial disclosure of traffic data

Each State Party shall adopt, in respect of traffic data that is to be preserved under Article 13, such legislative and other measures as may be necessary to:

a. ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and

b. ensure the expeditious disclosure to the State Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the State Party to identify the service providers and the path through which the communication was transmitted.

The powers and procedures referred to in this article shall be subject to Articles 20 and 21.

Article 15. Production order

Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a person in its territory in control of a computer system to produce from the system specified computer data or a printout or other intelligible output of that data; or

an Internet service provider offering its services in the territory of the State Party to produce information about persons who subscribe to or otherwise use the service.

The powers and procedures referred to in this article shall be subject to Articles 20 and 21.

Article 16. Search and Seizure

(1) Each State Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

a computer system or part of it and computer data stored therein; and

computer-data storage medium in which computer data may be stored in its territory.

(2) Each State Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1 (a), and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, such authorities shall be able to expeditiously extend the search or similar accessing to the other system.

Each State Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:

seize or similarly secure a computer system or part of it or a computer-data storage medium;

make and retain a copy of those computer data;

maintain the integrity of the relevant stored computer data; and

render inaccessible or remove those computer data in the accessed computer system.

(4) Each State Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.

The powers and procedures referred to in this article shall be subject to Articles 20 and 21.

Article 17. Lawful collection of traffic data

Each State Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:

collect or record through application of technical means on the territory of that Party, and

compel a service provider, within its existing technical capability, to:

collect or record through application of technical means on the territory of that Party, or

co-operate and assist the competent authorities in the collection or recording of,

traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.

(2) Where a State Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1, it may reserve the right not to apply, in whole or in part, paragraph 1.

Each State Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of and any information about the execution of any power provided for in this Article.

The powers and procedures referred to in this article shall be subject to Articles 20 and 21.

Article 18. Lawful interception of content data

Each State Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

a. collect or record through application of technical means on the territory of that Party, and

b. compel a service provider, within its existing technical capability, to:

i. collect or record through application of technical means on the territory of that Party, or

ii. co-operate and assist the competent authorities in the collection or recording of,

content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

(2) Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1, it may reserve the right not to apply, in whole or in part, paragraph 1.

Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of and any information about the execution of any power provided for in this Article.

The powers and procedures referred to in this article shall be subject to Articles 20 and 21.

Article 19. Use of forensic software

Each State Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to utilize a remote forensic software with the specific task required for the investigation and install it on the suspect's computer system in order to collect the relevant evidence.

Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1, it may reserve the right not to apply, in whole or in part, paragraph 1.

The powers and procedures referred to in this article shall be subject to Articles 20 and 21.

Article 20. Scope of procedural provisions

(1) Except as specifically otherwise provided in Articles 17, 18 and 19, each State Party shall apply the powers and procedures referred to in this Section to:

a. the criminal offences established in accordance with articles 3-12 of this Treaty;

b. other criminal offences committed by means of a computer system; and

c. the collection of evidence in electronic form of a criminal offence.

(2) Each Party may reserve the right to apply the measures referred to in Articles 17, 18 and 19 only to offences or categories of offences specified in the reservation.

Article 21. Conditions and safeguards

(1) Each State Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the applicable international human rights instruments, and which shall incorporate the principle of proportionality.

(2) Such conditions and safeguards shall, as appropriate in view of the nature of the power or procedure concerned, inter alia, include judicial or other independent supervision, grounds justifying application, and limitation on the scope and the duration of such power or procedure.

(3) To the extent that it is consistent with the public interest, in particular the sound administration of justice, a State Party shall consider the impact of the powers and procedures in this Section upon the rights, responsibilities and legitimate interests of third parties.

IV. JURISDICTION AND INTERNATIONAL COOPERATION

Traditional principles of jurisdiction are based on the territoriality which encompasses both the place of action and

the place where the result of an action occurs and nationality. Up to now, principles of jurisdiction for cybercrime offences are also committed to the traditional concept. With the transborder nature of cybercrime, there is still a lack of internationally recognized approaches which can establish «sufficient» link to apply territorial jurisdiction in the borderless Internet, when, for example, illegal content is offered on a server in one country and is accessible in many other countries. There are already some criteria suggested for establishing this link, such as: the location of data, the existence of any effect whatsoever in the prosecuting country, the existence of certain effects in the prosecuting country, the intention of the perpetrator to affect a certain country, or objective criteria such as language and topic in the case of illegal content. However, there is no international instruments that take into account the characteristic jurisdictional problems posed by international computer networks. The drafters of the Council of Europe Cybercrime Convention even refrained from including specific rules for criminal jurisdiction over satellites – although this was discussed – because a satisfactory solution can be derived from the general principles. Another drawback in existing approaches is that the international instruments contain no provisions for dealing with situations in which more than one state asserts or seeks to assert jurisdiction over a particular crime, and they create no new institutions that could solve these conflicts of jurisdiction [7].

Problems raised by conflicting jurisdictions in cyberspace are very complex and multi-faceted for finding appropriate solutions [8]. The interests of national governments in protecting sovereignty are still stronger than the motivation to find effective solutions for prosecution cybercrime. However, for tackling crime in global information networks the issue of jurisdiction shall be one of the outmost important problems to solve.

Another important issue is international cooperation. Despite the global nature of cybercrime, current approaches to international cooperation are based primarily on the cooperation of national authorities which means that cybercriminals can be always one step ahead – they operate in transborder networks, while mutual legal assistance between different countries requires time and official procedures. Outside the general work of Europol or Interpol, there are no special supranational or international institutions that deal specifically with cybercrime. Even if different international approaches to fighting cybercrime have already developed some instruments like 24/7 points of contact network, there is no real monitoring process assessing their implementation and effectiveness and im[proving them significantly. This is an indication that interest in the efficient prosecution of cybercrime has not surpassed the sovereignty interests of the collaborating states [9]. Development and implementation of the instruments for mutual legal assistance is a vital step to reach global consensus in cyberspace, because even with harmonization of substantive and procedural criminal law, without an effective international cooperation between states cybercrime investigations would not be effective.

V. OTHER INSTRUMENTS: SELF- AND CO-REGULATION

A recent trend in tackling cybercrime and maintaining cybersecurity is the involvement of different actors – both public and private – in the ecosystem of fighting cybercrime. This ecosystem nowadays consists increasingly of interdependent international and national actors linked to national information infrastructure networks and services, including financial and banking systems, energy supply and communications networks. The overall development and innovation of the ICT networks has been, and is largely, dominated and controlled by private actors. Broadband Internet is spreading faster than the rule of law. As a result, private rather than public actors often fund, manage and run an increasingly unruly Internet and communications networks. A policy dilemma is brewing, without clarity as to which entities can and should regulate and protect the cyberworld. This calls for new co-operative models of regulation and enforcement between governments and private industry on different levels – national, regional and international, and raises the challenge of developing effective approaches to co- and self- regulation to address offences in cyberspace.

While national governments have the power to establish and enforce legal and regulatory frameworks, the private sector understands the changing and converging nature of the ICT environment and has greater adaptability towards new technologies and services. Given the growing number of users and services, governments cannot and should not be expected to fight cybercrime alone because they have no resources to detect and stop every criminal infringement in cyberspace. Private actors have more expertise and resources, and possess the necessary knowledge to investigate cybercrime. The private sector's knowlegde and adaptability complement the resources and expertise of the government in the enforcement of regulations. That is why states are increasingly engaging in partnerships with the private sector to tackle cybercrime [10]; and co-regulatory and self-regulatory measures are sometimes appraised as being even more effective than criminal law and its enforcement [11]. Different types of private actors, including Internet Service Providers, e-commerce, m-commerce, e-payment companies, and application developers and vendors, become "critical nodes" in the cybercrime ecosystem for preventing and investigating cybercrime in their respective sectors [12]. This trend started in 1990s with the creation of the first private hotlines for reporting illegal content, especially child abuse. Nowadays self- and co-regulatory models are taken as an approach in many areas of fighting cybercrime both on national and international levels. This is why the development of the new legal frameworks shall include consultations with different stakeholders, including a range of various representatives of the private industry. In addition, reaching consensus on self- and co-regulation and transferring the best practices in this field from

the national level to the international can significantly contribute the effort of international community to tackle cybercrime. Self- and co-regulation can not replace the proper legal frameworks but it can complement them in order to make them more successful.

VI. Conclusion

Cybercrime impacts many areas of law. Thus, drafting legal framework for cybercrime legislation is, first of all, more complex that for any other types of crime, and, secondly, shall include the study of the process of legal harmonisation, its factors, forces and the agents of change, as well as gap assessment. This analysis shall take into account the complexity of cybercrime, the new challenges emerging in cyberspace with further development of the information technologies, such as botnet attacks or cloud computing, and the tensions between traditional criminal law and transborder computer offences.

On the national and international levels, legal reform addressing the challenges of crime in cyberspace is being developed in several areas, which create the structure gap assessment and identification of the areas requiring special attention in the process of harmonisation of cybercrime legislation.

The key factor for approaching consensus on legal framework is collaboration between different international organizations and national governments. There is no lack of approaches to tackle cybercrime. The gap assessment that is currently being done by various international organisations and national governments in order to detect the loopholes in current state of cybercrime legislation in different jurisdictions, to identify the best approaches to criminalise offences and to improve the global agenda to tackle the phenomena of crime in global information networks represents the basis for achieving the global harmonisation. Cooperation between those bodies can enhance mutual efforts in achieving the main goal – peace and security in cyberspace.

References

[1] For detailed analysis why the role of organized crime groups is likely to increase see: Gercke, M. "Cyberrcime". Chapter 10 in UNODC, The Globalization of Crime. A Transnational Organized Crime Threat Assessment. 2010. 203-220

[2] Gercke, M., Tropina, T., Lozanova, Y. and Sund, C. The role of ICT regulation in addressing offenses in cyberspace. GSR10 Discussion Paper. ITU, 2011. P. 3.

[3] Yeo, Lack of cybercrime laws impedes Asia's cross-border efforts?, available at: www.zdnetasia.com/lack-of-cybercrime-laws-impedes-asia-s-cross-border-efforts-62040170.htm

[4] ITU, Cybersecurity Guide for Developing Countries. ITU, 2009, available at: www.itu.int/ITU-D/cyb/publications/2009/cgdc-2009-e.pdf.

[5] For the reasons why Cybercrime Convention has not reached international success see: Gercke, M. «10 years Convention on Cybercrime - Achievements and Failures of the Council of Europe´s Instrument in the fight against Inter-related Crimes» in Computer Law Review International, Issue 5 15. October 2011, page 129-160

[6] Gercke M., Tropina, T. "From Telecommunicaiton Standardisation to Cybercrime Harmonisation? ITU Toolkit for Cybercrime Legislation" in Computer Law Review International, Issue 5, 2009, P. 138

[7] Sieber, U. "Mastering Complexity in the Global Cyberspace: The Harmonization of Computer-Related Criminal Law" in: Delmas-Marty, M. / Pieth, M. / Sieber, U. (ed(s).): Les chemins de l'Harmonisation Pénale/Harmonising Criminal Law, Collection de L'UMR de Droit Comparé de Paris, Bd. 15. Paris, Société de législation comparée, 2008, p. 127 - 202.

[8] S.W. Brenner, "Cybercrime and Jurisdiction", B.-J. Koops, S.W. Brenner (eds.), The Hague, Asser Press, 2006, pp. 327-354.

[9] Sieber, ibid.

[10] See Sahel, J., A new policy-making paradigm for the Information Society, TPRC conference, 2006. Available at: <http://web.si.umich.edu/tprc/papers/2006/635/NewParadigmInfoSociety.pdf>; Marsden, C., at al. Options for an Effectiveness of Internet Self- and Co-Regulation. Phase 1 Report: Mapping Existing Co- and Self-Regulatory Institutions on the Internet. RAND Europe Available at: <http://ec.europa.eu/dgs/information_society/evaluation/data/pdf/studies/s2006_05/phase1.pdf>

[11] Sieber, ibid

[12] OECD, The Role of Internet Intermediaries in Advancing Public Policy Objectives. OECD Publishing, 2011, P. 196.