INTERNATIONAL AND REGIONAL ORGANIZATIONS WITH ATTRIBUTES AND PREOCCUPATIONS IN PREVENTING AND FIGHTING AGAINST CYBERCRIME AND THEIR MAIN ACCOMPLISHMENTS

Gheorghe-Iulian Ioniță[1]
Ștefania-Diana Ioniță-Burda[2]

Abstract

At global level, there are various organizations which are constantly concerned with the analysis of the latest manifestations and evolution of cybercrime, setting up work groups to develop strategies for the prevention and fight of cybercrimes. Besides these international organizations which act globally, several other organizations focus on certain regions, dealing with issues related to cybercrime.

Keywords: cybercrime, organizations, declaration, resolution, convention

1. United Nation (UN)

United Nation (UN)[i] is an international organization founded in 1945 after the Second World War by 51 countries committed to maintaining international peace and security, developing friendly relations among nations and promoting social progress, better living standards and human rights; currently, almost all nations of the world are UN members, i.e. 193 countries in all.

In **1990**, at the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders (Havana, Cuba, 27 August - 7 September 1990), the General Assembly adopted a resolution regarding cybercrime legislation, **A/RES/45/121**[ii], under which the UN published in 1994, United Nations Manual on the prevention and control of computer-related crime[iii].

In **2000**, the General Assembly adopted a resolution on **Combating the criminal misuse of information technologies**, **A/RES/55/63**[iv], where it identified a series of measures meant to prevent the misuse of information technology.

In **2001**, the General Assembly adopted another resolution on **Combating the criminal misuse of information technologies**, **A/RES/56/121**[v], which refers to the existing international approaches in their fight against cybercrime and highlights various solutions:

„*Noting* the work of international and regional organizations in combating hightechnology crime, including the work of the Council of Europe in elaborating the Convention on Cybercrime, as well as the work of those organizations in promoting dialogue between government and the private sector on safety and confidence in cyberspace,

[1] PhD., Lecturer of Criminal Law at the Romanian American University in Bucharest. E-mail: ionita.gheorghe.iulian@profesor.rau.ro
[2] PhD. Candidate, Lecturer of Labor Law at the Romanian American University in Bucharest. E-mail: ionitaburda.stefania.diana@profesor.rau.ro

1. *Invites* Member States, when developing national law, policy and practice to combat the criminal misuse of information technologies, to take into account, as appropriate, the work and achievements of the Commission on Crime Prevention and Criminal Justice and of other international and regional organizations;

2. *Takes note* of the value of the measures set forth in its resolution 55/63, and again invites Member States to take them into account in their efforts to combat the criminal misuse of information technologies;

3. *Decides* to defer consideration of this subject, pending work envisioned in the plan of action against high-technology and computer-related crime of the Commission on Crime Prevention and Criminal Justice".

In **2005**, at the Eleventh United Nations Congress on Crime Prevention and Criminal Justice in Bangkok, Thailand, was adopted a declaration[vi] „**Synergies and Responses: Strategic Alliances in Crime Prevention and Criminal Justice**", which stressed the harmonization need in cybercrime fight:

„… 14. Mindful of General Assembly resolution 59/156 of 20 December 2004, on preventing, combating and punishing trafficking in human organs, we note the serious concerns raised about the illicit removal of and trafficking in human organs and will examine with interest the report of the Secretary-General requested in that resolution.

15. We reaffirm the fundamental importance of implementation of existing instruments and the further development of national measures and international cooperation in criminal matters, such as consideration of strengthening and augmenting measures, in particular against cybercrime, money-laundering and trafficking in cultural property, as well as on extradition, mutual legal assistance and the confiscation, recovery and return of proceeds of crime …".

2. Group of Eight (G8)

Group of Eight (**G8**), and formerly the **G6,** then **G7**, is a forum, created by France in 1975, for the governments of seven major economies: Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States. In 1997, the group added Russia, thus becoming the G8.

In **1997**, on the occasion of the ***meeting of ministers of justice and internal affairs*** of G8 (Washington, DC, December 10)[vii], the "**Principles and Action plan for fighting high-tech crime**" were adopted, with ten points each, that were approved subsequently.

A. ***The Declaration of principles*** contains, among others:

"There must be no safe havens for those who abuse information technologies.

Investigation and prosecution of international high-tech crimes must be coordinated among all concerned States, regardless of where harm has occurred. Law enforcement personnel must be trained and equipped to address high-tech crimes. Legal systems must protect the

confidentiality, integrity, and availability of data and systems from unauthorized impairment and ensure that serious abuse is penalized.

Legal systems should permit the preservation of and quick access to electronic data, which are often critical to the successful investigation of crime".

B. ***The Action plan*** (to support the principles) contains, among others:
„…Take appropriate steps to ensure that a sufficient number of trained and equipped law enforcement personnel are allocated to the task of combating high-tech crime and assisting law enforcement agencies of other States.

Review our legal systems to ensure that they appropriately criminalize abuses of telecommunications and computer systems and promote the investigation of high-tech crimes …
Develop and employ compatible forensic standards for retrieving and authenticating electronic data for use in criminal investigations and prosecutions".

In **1999**, at Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime (Moscow, October 19-20)[viii], G8 specified (point 14-23 of the Conference release) their plans regarding high-tech crimes. Thus, they expressed their position regarding High-tech crime (pct. 14-15), strength of G-8 Legal Systems (pct. 16), principles on transborder access to stored computer data (pct. 17), etc. A series of principles in the fight against cybercrime adopted on this occasion are still to be found in a series of international strategies.

In **2001**, on the occasion of the ***meeting of ministers of justice and internal affairs*** of G8 (Milan, 26-27 February 2001)[ix] debates were held on the topic of actions against high-tech crime, including use of the Internet in child pornography, were debated upon (among others), with emphasis (in the Conference release) on the need to complete the European Council Convention on cybercrime.

In **2004**, on the occasion of the ***meeting of ministers of justice and internal affairs*** of G8 (Washington DC, May 11)[x], "C**ombating Cybercrime and Enhancing Cyber Investigations**" was one of the major concerns, participants stressing (in the Conference release) the infrastructure protection and the best practices. On this occasion, the "**Best Practices For Network Security, Incident Response And Reporting To Law Enforcement**"[xi] were presented as developed by the G8's Subgroup on High-Tech Crime to assist network operators and system administrators when responding to computer incidents.

In **2006**, upon the G8 ***Summit*** (St. Petersburg, July 16), the problem of computer terrorism was discussed, reasserting (point of the **Reunion statement)**[xii] the involvement in „…effectively countering attempts to misuse cyberspace for terrorist purposes, including incitement to commit terrorist acts, to communicate and plan terrorist acts, as well as recruitment and training of terrorists".

In **2008**, on the occasion of the ***meeting of ministers of justice and internal affairs*** of G8 (Tokyo, June 13)[xiii], the term "ID-Related Crime" was launched (in the **Final statement),**

specifying that „… is not a formal legal concept, and here it is meant to broadly cover unlawful conduct involving abuse of identities. It includes falsification, alteration, as well as unauthorized acquisition, transfer, possession or use of identification documents and identification information …".

3. International Telecommunication Union (ITU)

International Telecommunication Union (ITU)[xiv], is the United Nations specialized agency for information and communication technologies – ICTs which, with 193 member states, plays an essential role in developing and standardizing telecommunications, as well as information security issues.

It is worth mentioning that ITU held a vital role in the organization of the **World Summit on the Information Society** (WSIS), due to the Resolution of the General Assembly **A/RES/56/183**[xv], which comprised two stages [xvi]:

Geneva, December 10-12, 2003, whose objective was to develop and foster a clear statement of political will and take concrete steps to establish the foundations for an Information Society for all, reflecting all the different interests at stake;

Tunis, November 16-18, 2005, whose objective was to put Geneva's Plan of Action into motion as well as to find solutions and reach agreements in the fields of Internet governance, financing mechanisms, and follow-up and implementation of the Geneva and Tunis documents. Governments, politicians and experts worldwide exchanged ideas and experiences regarding the best way to approach the emerging issues associated with the development of a global information society, including the development of compatible standards and laws. The Reunion results are contained in the Geneva Declaration of Principles[xvii] Geneva Plan of Action[xviii]; Tunis Commitment[xix] and Tunis Agenda for the Information Society [xx].

A. The ***Geneva Plan of Action*** stresses the significance of measures in the fight against cybercrime:

„… C5. **Building confidence and security in the use of ICTs …** 12. Confidence and security are among the main pillars of the Information Society. … Governments, in cooperation with the private sector, should prevent, detect and respond to cyber-crime and misuse of ICTs by: developing guidelines that take into account ongoing efforts in these areas; considering legislation that allows for effective investigation and prosecution of misuse; promoting effective mutual assistance efforts; strengthening institutional support at the international level for preventing, detecting and recovering from such incidents; and encouraging education and raising awareness ...".

B. The ***Tunis Agenda for the Information Society*** underlines the need of international cooperation for fighting against cybercrime and refers to existing legislative approaches:

„… **40. We underline** the importance of the prosecution of cybercrime, including cybercrime committed in one jurisdiction, but having effects in another. **We further underline** the necessity of effective and efficient tools and actions, at national and international levels, to

promote international cooperation among, *inter alia*, law-enforcement agencies on cybercrime. **We call upon governments** in cooperation with other stakeholders to develop necessary legislation for the investigation and prosecution of cybercrime, noting existing frameworks, for example, UNGA Resolutions 55/63 and 56/121 on "*Combating the criminal misuse of information technologies*" and regional initiatives including, but not limited to, the Council of Europe's *Convention on Cybercrime* …".

Following the WSIS, ITU was appointed as sole facilitator for the C5 action line dedicated to building trust and security in the use of information technology and communications. In 2007, the ITU general secretary launched the Global Agenda on Information Security (GCA).

The ITU Global Cybersecurity Agenda (GCA)[xxi] *is built upon five strategic pillars – Legal Measures, Technical and Procedural Measures, Organizational Structures, Capacity Building, International Cooperation – and made up of seven main strategic goals:*

„1. Elaboration of strategies for the development of a **model cybercrime legislation** that is globally applicable and interoperable with existing national and regional legislative measures.

2. Elaboration of global strategies for the creation of appropriate national and regional **organizational structures** and policies on **cybercrime**.

3. Development of a strategy for the establishment of globally accepted minimum **security criteria and accreditation schemes for hardware and software applications and systems**.

4. Development of strategies for the creation of a global framework for **watch, warning and incident response** to ensure cross-border coordination between new and existing initiatives.

5. Development of global strategies for the creation and endorsement of a **generic and universal digital identity system** and the necessary **organizational structures** to ensure the recognition of digital credentials across geographical boundaries.

6. Development of a *global strategy to facilitate* **human and institutional capacity building** to enhance knowledge and know-how across sectors and in all the above-mentioned areas.

7. Proposals on a framework for a *global multi-stakeholder strategy* for **international cooperation, dialogue and coordination** in all the above-mentioned areas".

4. European Council (CoE)

European Council (CoE)[xxii] is an inter-governmental organization with 47 member states (out of which 27 are EU members).

In **1976**, *the problem of cybercrime* was discussed by the European Council at the 12th Conference of Managers of Forensics Research Institutes[xxiii] and *mentioned* as an *unspecified crime* in the Recommendation project for economic crime adopted by the Council of Ministers on its 335th meeting of June 25, **1981**, under no. ***R (81) 12***[xxiv].

In **1985**, *the problem of cybercrime* was included[xxv] on the agenda of the European Committee for Penal Problems (CDPC) for 1985-1986, the Committee appointing a Commission of Cybercrime Experts (PC-R-CC) to study this problem. The Commission

started its activity in 1985 and completed it in March 1989. At the last meeting, the Commission adopted the report of a recommendation project that was sent to the Committee for approval. The recommendation project and the report were adopted by the Committee in June 1989 and by the Council of Ministers on its 428th meeting of September 13, **1989**, under no. ***R (89) 9***[xxvi].

In **1995**, the Council of Ministers, on the 543rd meeting of deputy minister of September 11, adopted another recommendation project on the problems of penal law with respect to cybercrime, under no. ***R (95) 13***[xxvii].

In **1996**, based on pragmatic consideration, the European Committee on Crime Problems (CDPC) decided (decision CDPC/103/211196) to set up a committee of experts to deal with cyber-crime. Further to this decision, the Committee of Ministers set up the new committee, called "the Committee of Experts on Crime in Cyber-space (PC-CY)" by decision n° CM/Del/Dec(97)583, taken at the 583rd meeting of the Ministers' Deputies, held on 4 February 1997. Between 1997 and 2000, the Committee PC-CY held 10 meetings in plenary and 15 meetings of its open-ended Drafting Group.

The revised and finalized draft Convention and its Explanatory Memorandum were submitted for approval to the CDPC at its 50th plenary session in June 2001, following which the text of the draft Convention was submitted to the Committee of Ministers for adoption and opening for signature[xxviii].

At the execution ceremony held in Budapest on November 23, 2001, 30 countries signed the European Council Convention on cybercrime[xxix] (including four non member states of the European Council, i.e. Canada, United States of America, Japan and South Africa, that attended the negotiations). Currently, 47 countries signed the Convention, out of which 32 adhered to it.

In **2003**, the Convention was followed by Additional Protocol concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems[xxx], Strasbourg, January 28.

During the negotiations on the Convention text, it seemed that the indictment of the dissemination of racist and xenophobic materials was the main controversial issue. Some countries, which adopted a strong protection of the free speech principle, expressed their concern that, if the Convention includes provisions which prevent free speech, it would be impossible for them to sign the Convention; consequently, such aspects were integrated separately in this protocol.

5. European Union (EU)

European Union (EU)[xxxi] is a unique economic and political partnership between 27 European countries.

In **1999**, the European Union launched the initiative "eEurope", by adopting the Communicate of the European Commission "eEurope 2005: An information society for all"[xxxii], under which Europe must have basic services with electronic access by 2005.

In **2001**, the European Commission published a paper called "***Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime***"[xxxiii]. In this paper, the Commission analyzed and approached the issue of cybercrime and highlighted the need for efficient measures to cope with threats to the integrity, availability and viability of computer systems ad networks.

„Information and communication infrastructures have become a critical part of our economies. Unfortunately, these infrastructures have their own vulnerabilities and offer new opportunities for criminal conduct. These criminal activities may take a large variety of forms and may cross many borders. Although, for a number of reasons, there are no reliable statistics, there is little doubt that these offences constitute a threat to industry investment and assets, and to safety and confidence in the information society.

Measures may be taken both with respect to the prevention of criminal activity by strengthening the infrastructures of information security and by ensuring that law enforcing authorities have the appropriate means to act and, at the same time, to comply with fundamental human rights. The commission that participated in both discussions, in the European Council and G8, admits the complexity and difficulties related to aspects of procedural law. But the efficient cooperation within the EU for fighting cybercrime is an essential element for a safe information society and for creating a space of freedom, security and justice …".

In **2007**, the European Commission published a document called "***Towards a general policy on the fight against cyber crime***"[xxxiv], which specifies as its general strategic objective the "strengthening of cybercrime at national, European and international level", an objective which can be further divided into three operational directions:

„- improving and facilitating coordination and cooperation between the units of cybercrime prevention, relevant authorities and other EU experts

- developing, together with member states, relevant European and international organizations and other interested parties, a coherent framework of EU policies of cybercrime prevention

- increasing awareness of costs and dangers represented by cybercrime".

---

i United Nation (UN), at http://www.un.org.

ii United Nation, General Assembly, A/RES/45/121, at http://www.un.org/documents/ga/res/45/a45r121.htm.

iii United Nation Office at Vienna. Centre for Social development and Humainitarian Affair, United Nation Manual on the prevention and control of computer-related crime, în International Review of Criminal Policy, no. 43 şi 44 (September), 1994, at http://www.uncjin.org/Documents/EighthCongress.html.

iv United Nation, General Assembly, A/RES/55/63, at http://www.unodc.org/pdf/crime/a_res_55/res5563e.pdf.

v United Nation, General Assembly, A/RES/56/121, at http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_56_121.pdf.

vi UN, Bangkok Declaration, Synergies and Responses: Strategic Alliances in Crime Prevention and Criminal Justice, at http://www.unodc.org/pdf/crime/congress11/BangkokDeclaration.pdf.

vii G8 Information Centre, G8 Justice and Interior Ministers, at http://www.g8.utoronto.ca/justice/index.html.

viii Ministerial Conference of the G-8 Countries on Combating Transnational Organized Crime, (Moscow, October 19-20, 1999), at http://www.g8.utoronto.ca/adhoc/crime99.htm.
ix Conference of the G8 Ministers of Justice and Interior, Milano, 26-27 February 2001, at http://www.g8.utoronto.ca/adhoc/justice2001.htm.
x G8 Justice and Home Affair, Washington DC, May 11, 2004, at http://www.g8.utoronto.ca/justice/justice040511_comm.htm.
xi G8's Subgroup on High-Tech Crime, Best Practices for Network Security, Incident Response and Reporting to Law Enforcement, at http://www.g8.utoronto.ca/justice/G8justice2004_networks.pdf.
xii G8 Summit Declaration on Counter-Terrorism, St. Petersburg, July 16, 2006, at http://www.g8.utoronto.ca/summit/2006stpetersburg/counterterrorism.html.
xiii G8 Ministers of Justice and Interior, Tokyo, June 13, 2008, at http://www.g8.utoronto.ca/justice/justice2008.htm.
xiv International Telecommunication Union (ITU), at http://itu.int.
xv United Nation, General Assembly, A/RES/56/183, at http://www.un-documents.net/a56r183.htm.
xvi World Information Summit on the Information Society (WSIS), at http://www.itu.int/wsis/basic/about.html.
xvii WSIS-03/GENEVA/DOC/4-E, Declaration of Principles: Building the Information Society: a global challenge in the new Millennium, at http://www.itu.int/wsis/docs/geneva/official/dop.html.
xviii WSIS-03/GENEVA/DOC/5-E, Plan of Action, at http://www.itu.int/wsis/docs/geneva/official/poa.html.
xix WSIS-05/TUNIS/DOC/7-E, Tunis Commitment, at http://www.itu.int/wsis/docs2/tunis/off/7.html.
xx WSIS-05/TUNIS/DOC/6(Rev.1)-E, Tunis Agenda for The Information Society, at http://www.itu.int/wsis/docs2/tunis/off/6rev1.html.
xxi The ITU Global Cybersecurity Agenda (GCA), at http://www.itu.int/osg/csd/cybersecurity/gca/pillars-goals/index.html.
xxii Council of Europe (CoE), at http://www.coe.int/.
xxiii Twelfth Conference of Directors of Criminological Research Institutes: Criminological Aspects of Economic Crime, Strasbourg, 1976.
xxiv Council of Europe, Committee of Ministers, Recommendation no. R (81) 12 of Committee of Ministers to Member States on Economic Crime (adopted by the Committee of Ministers on 25 June 1981 at the 335th meeting of the Minister's Deputies).
xxv Council of Europe, Computer-related Crime, Recommendation No. R (89) 9 on computer-related crime and final report of the European Committie on Crime Problems, Council of Europe Publishing and Documentation Service, Strasbourg, 1990, p. 9.
xxvi Council of Europe, Committee of Ministers, Recommendation no. R (89) 9 of Committee of Ministers to Member States on Computer-Related Crime (adopted by the Committee of Ministers on 13 September 1989 at the 428th meeting of the Minister's Deputies).
xxvii Council of Europe, Committee of Ministers, Recommendation no. R (95) 13 of Committee of Ministers to Member States on Computer-Related Crime (adopted by the Committee of Ministers on 11 September 1995 at the 543th meeting of the Minister's Deputies).
xxviii Council of Europe, Convention on Cybercrime (ETS No. 185) Explanatory Report, section 7, 12, 13, 15, at http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.
xxix Council of Europe, Convention on Cybercrime (CETS no: 185), at http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.
xxx Council of Europe, Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS no. 189), at http://www.conventions.coe.int/Treaty/EN/Treaties/Html/189.htm.
xxxi European Union (UE), at http://europa.eu.
xxxii Commission of The European Communities, Communication from The Commission to The Council, The European Parliament, The Economic and Social Committee and The Committee of The Regions, eEurope 2005: An information society for all, COM (2002) 263, Brussels, 2002, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2002:0263:FIN:EN:PDF.
xxxiii Commission of The European Communities, Communication from The Commission to The Council, The European Parliament, The Economic and Social Committee and The Committee of The Regions, Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, COM (2000) 890, at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2000:0890:FIN:EN:PDF.
xxxiv Commission of The European Communities, Communication from The Commission to The European Parliament, The Council and The Committee of The Regions, Toward a general policy on the fight against cyber

crime, COM (2007) 267 final, at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF.