ул. "Дякон Игнатий" № 9, София 1000
Република България
тел: (+359 2) 940 9771;
факс (+359 2) 988 5094

Доклад за обсъжданите теми и резултатите на конференцията „Октопод" на Съвета на Европа

Предварителна бележка

От 21 до 22 ноември 2011 г. в Страсбург се състоя конференцията „Октопод" на Съвета на Европа, посветена на борбата срещу престъпленията в мрежата. Основен инструмент за предотвратяване на атаките и посегателствата в Интернет е Конвенцията на Съвета на Европа срещу киберпрестъпленията, наричана още Будапещенска конвенция. На 23 ноември 2011 г. се навършиха десет години от подписването ѝ, събитие, на което беше посветено тържествено заседание, открито от генералния секретар на организацията Торнбьорн Ягланд. В заключение Комитетът по Конвенцията срещу киберпрестъпленията (TC-Y) проведе своето пленарно заседание и прие план за действие.

Следва докладът на Бисера Занкова, медиен консултант към МТИТС, която участва в конференцията и в заседанията като представител на Управителния комитет по медии и нови комуникационни услуги на Съвета на Европа (CDMC).

A special item on the Council of Europe agenda in November 2011 was the Octopus Conference which was dedicated not only to fostering international cooperation against cybercrime (a traditional theme for the Octopus conferences so far) but to the merits, achievements and enlargement of the Council of Europe Convention on Cybercrime (Budapest convention). In this way the discussions about the most effective responses to crimes in cyber space were connected to the celebrations of the 10th anniversary of the Budapest Convention signed on November 23 2001 in Budapest.

The Octopus Conference is part of the Global Project on Cybercrime which is currently funded by voluntary contributions from Estonia, Japan, Monaco, Romania, Microsoft and VISA Europe as well as the budget of the Council of Europe.

The conference was opened by **Mr. Jan Kleijssen, Director of Information Society and Action against Crime** at **the Council of Europe**, who in his opening remarks clearly stated that the fight against cybercrime is a priority for the Council of Europe. He emphasized the importance of the international cooperation in this respect and pointed to the necessity of applying a whole range of related standards and tools for the protection of human rights. With regard to this Mr. Kleijssen mentioned the data protection convention of the Council of Europe and the need to promote it among states together with the Budapest convention. Further in his address Mr. Kleijssen referred to the conference which had taken place in early November 2011 in London (http://www.huffingtonpost.com/2011/11/01/london-conference-on-cyberspace_n_1069331.html) the conclusions of which regarding enhanced international cooperation against cybercrime and the effective protection of human rights in cyber space could be considered directly related to the Octopus debates.

Министерство на транспорта, информационните технологии и съобщенията на Република България 2014 Всички права запазени
Министерство на транспорта, информационните технологии и съобщенията

Ms. Eleonor Fuller, Permanent Representative of the UK to **the Council of Europe** provided more detailed information about the London conference. In her expose Ambassador Fuller dwelled on a number of benefits of the Internet which had to be preserved and expanded in the new technological environment – economic growth, job benefits, safe access and international security. She put particular stress on the fact that cybercrime jeopardizes economic systems worldwide and that is why in the fight against this global threat international cooperation is vital. The UK ambassador did not miss the opportunity to reassure all participants and guests that the fight against cybercrime and the signing and ratifying of the Budapest convention are two interrelated priorities of the UK chairmanship of the Council of Europe.

Mr. Hiroshi Kanebe, Consul Gneral, Permanent Observer of Japan to **the Council of Europe**, expressed his appreciation of the ten successful years of operation of the Budapest convention as an instrument which provides the basis for secure and safe cyber environment. He stressed the global nature of cybercrime posing threats for every country, institution and person around the globe. Against such a background domestic efforts would not be sufficient to remove the risks of cyber attacks and international collaboration remains the essential core of the whole system of fight and protection.

The official part of the opening session ended with the formulation of several important objectives:

» We all need safe cyberspace so that it can fulfill its potential;

» All sectors support trusted and secure cyber environment and there is a wide array of stakeholders that can cooperate for the accomplishment of this highly relevant goal;

» The Octopus conference is a long-term project which will develop with the support of different stakeholders, by itself it represents the success of real and effective international cooperation (Hungary and South Korea have proposed to be the hosts of the next two Octopus conferences).

The second part of the opening session focused on the one hand, on various aspects of cybercrime and on cybercrime legislation and its implementation, on the other. Abundant statistics were presented concerning the expansion of crime in cyberspace and the rapid increase of risks on line. Currently three times as many adults suffer cybercrime than crime in an offline environment, 114 bln dollars are the actual loss of cybercrime, 431 incidents happen per year and 14 per second. On the other hand, the habits and the knowledge of the population are inadequate to counteract the damaging effects of cybercrime – nearly half of the population working on the computer does not apply security control and only 2 out of 10 walk to the law enforcement units to report cyber attacks. All these figures raise concern about the education and the confidence of Internet users.

Another serious problem in cyber space is the sexual exploitation and abuse of children. Reasons are complex however, some of the difficulties stem from the conditions that much more static legal systems have to catch up with the rapidly changing communications environment with all its benefits and risks.

Nicola di Leone from High - Tech crime Centre Europol reminded that cybercrime targeting citizens represented a multidimensional threat and cyber attacks became more and more sophisticated being launched by a new generation of criminals. Complications in combating crime on the net are due by and large to jurisdiction, the regulation of which is lagging behind, the international investigations which are converging and the large amount of data and evidence has to be processed. All these challenges require a number of measures - common strategies with Interpol and other organizations to be established, networks with the private sector to be build, a new concept of data protection under the conditions of cloud

Министерство на транспорта, информационните технологии и съобщенията на Република България 2014 Всички права запазени
Министерство на транспорта, информационните технологии и съобщенията

computing to be formulated and cross-border instruments for investigation to be elaborated.

Demosthenes Ikonomou, Team Leader of the Mobile Assistance Team, ENISA, focused particularly on the situation in Europe. He underlined that Europe represented by public bodies, by the private sector, by its agencies and citizens was under huge attack as cybercrime is not confined to boundaries or states. ENISA (the European Network and Information Security Agency) was created to serve the EU public sector and more particularly to advise European Commission and member states on information security, to collect and analyze data on security practices and to promote cooperation. A new area in the activities of the agency is to safeguard privacy and to promote trust in future information systems. Cybersecurity in a global environment as a highly desirable goal is a shared responsibility. It requires structured policy approach at an international level aligning policy and objectives to different communities. Especially for Europe such an approach means coherent policy within its borders aligned to the aims of its partners. For the successful application of the new approach governance will be a key issue both within and out of the borders of the EU. ENISA will work for the achievement of these goals from a legal and regulatory perspective and by facilitating dialogue – within the EU and globally.

Vincent Hinderer, CERT-LEXSI, France, presented the CERT perspective to cybercrime problems. There are 250 computer emergency response teams that can exchange information. Their aim is to raise awareness and to secure coding and contracting. CERT's key-asset is to build a trust cooperation network.

The activities of the **Cybercrime Convention Committee (T - CY)** were described by **Markko Kunapu, Chair of the committee, Ministry of Justice of Estonia**. According to Mr. Kunappu modern developments present various challenges and responses to at least three issues have to be found most urgently – the transborder access to data, the improvement of the accession process to the Budapest convention and the introduction of possible amendments to the instrument by attaching a protocol for solving jurisdictional problems.

The final exchange of the morning plenary session focused on the recent situation in Africa, Asia/Pacific and the Americas with respect to their preparedness to join the Budapest convention. Delegates from Argentina, Benin, Botswana, India, Indonesia, Nigeria, Niger, Pakistan, Paraguay, Peru, Philippines, Tanzania, Tonga, Kambodja, Russia and Uzbekistan made short interventions about the state of their national legislation.

The information about the new Indian InfoTech act sounded really encouraging. The law benefits immensely from the Council of Europe standards and follows closely the constantly evolving environment. The amendments to the law from 2008/2009 increased the applicability of the existing act and put it in compliance with the Council of Europe Cybercrime Convention. Under the new provisions which are technology neutral monitoring and collecting of traffic data can be done by any type of device and the intermediaries have to follow reasonable security practices. The scope of the law has been widened to cover child pornography. The act also gives government the power to adopt rules starting from April 2011. The first broad rules passed concerned the duties and obligations of the intermediaries and sensitive data.

The afternoon session during the first day of the Octopus conference began with two parallel workshop sessions – one dealing with capacity building and another concentrating on specialized services.

The session on capacity building presented various projects related to the fight against cybercrime which through effective collaboration could enhance the results pursued. The projects as such usually concentrate on fostering the reform processes in different countries which aim at bringing the domestic legislation in line with the Budapest convention and at integrating and consolidating international efforts in this respect. Among the initiatives discussed were the projects of the Council of Europe and the European Union – **the CyberCrime@IPA and the CyberCrime@EAP**; **the Commonwealth Cybercrime Initiative** the purpose of which is to develop substantive capacity around CW countries; **UNODC** (UN

Министерство на транспорта, информационните технологии и съобщенията на Република България 2014 Всички права запазени
Министерство на транспорта, информационните технологии и съобщенията

Office on Drugs and Crime) which pursues complex activities against cybercrime and organized crime and serves as an example of global action in the field through its cooperation with ITU; seminars on **judicial training in UK, Malaysia and France**; models of **law enforcement capacity building** in Ireland and the Netherlands and **workshops** carried out in Pacific Island and Sri Lanka as part of the Global Project on Cybercrime of the Council of Europe.

The second day of the Octopus conference was dedicated to two central issues – the cybercrime strategies and the responses to the sexual exploitation of children.

The workshop which dealt with the sexual exploitation and abuse of children discussed thoroughly both criminal law and preventive measures. In her paper on substantive law benchmarks **Ms. Cristina Schulman, Head of Cybercrime Unit, Council of Europe** emphasized the complexity of the policy against sexual exploitation of children which had to be implemented by the states. The Council of Europe convention is helpful in this respect as it can be a sound basis for the elaboration of a comprehensive framework. Many different tools can be deployed for the effective protection of children in cyberspace, however, criminal law measures remain the most important among them. Ms. Schulman underlined the significance of the Budapest convention for raising awareness among the public about the risks on the Internet. She stressed particularly the necessity of consistent work on cooperation projects against cybercrime.

The experience of the **Virtual Global Task Force, Australian Federal Police** was presented by **Neil Gaughan, Chair of the Task Force.** He explained that the aim of the project is to stop sexual assault against children and it unites a large number of NGOs involving in practice the whole community. One of the main goals pursued is to help victims by making them speak out about the abuse they have suffered. The task force counts on the concerted efforts of the law enforcement key-players and civil society organizations. Through close collaboration stakeholders aim at the destruction of the illegal material. Essential for the success of the actions is the civil participation and commitment.

In her expose **Ms. Samantha Woolfe** from **ICMEC (the International Centre for Missing and Exploited Children)** spoke in favour of harmonized legislation which could be considered crucial for successful combating child abuse and sexual exploitation. Two hundred images of child pornography are posted daily online and these images become even more graphic and violent. ICMEC has prepared model legislation in 2006 which is in place in 196 countries. One of the issues that should be considered in greater detail at international fora is whether a new definition of child pornography is needed. Different legal solutions are in force in various countries – in Scandinavia for instance, sexual exploitation is differentiated from abuse, while in the USA what matters for prosecution authorities is what actually has happened to the child. When discussing the problem of child pornography it is important to be born in mind that perpetrators are stimulated by the images to abuse children. What is depicted there does not necessarily exist in reality. Another tough issue is that very rarely investigative bodies have evidence about the real identity of the child. Therefore laws generally have to cope with such a variety of hard problems and to suggest workable solutions.

In the course of the debates in this panel participants discussed the EU directive on combating child sexual abuse and exploitation. **Ms. Cathrin Bauer-Bulst, Policy Officer, DG Home, EC** spoke about the new trends provided by the EU directive. She referred particularly to the removal of pornographic content which is an obligation of member states. Blocking is a complementary measure and can take place under procedural safeguards including the right of judicial review. The directive envisages improved procedure of notice and take down which is still considered an important measure but not the only one in this respect. The purpose is to track the illegal content more effectively. For instance, if taken down images appear again, other opportunities to take them down are applied including technical ways. MICROSOFT and ICANN are valuable partners in such operations. Ms. Bauer-Bulst informed about the EC funding of several projects in the field one of which is about the identification system of the victims of child pornography. She concluded that the new EU directive is a compromise reached

Министерство на транспорта, информационните технологии и съобщенията на Република България 2014 Всички права запазени
Министерство на транспорта, информационните технологии и съобщенията

between 27 member states; the act is far from being considered the ideal instrument in this sensitive area as many issues concerning its practical implementation have still to be clarified.

The topic about the activities of the hot-lines was also present in the discussions of the workshop. **Mr. John Carr from the European NGO Alliance for Child Safety Online, Denmark** shared his views about the notice and take down procedure applied by the hotlines. Nowadays the notice and take down approach is an unalienable element of any strategy that deals with child abuse. Usually hotlines work together with the local law enforcement agencies. They do not do any investigation what so ever but refer the signals to the police. There are hotlines, however that issue the take and down notice themselves. The British way of handling the mater is to inform the hotlines about the illegal content and then the hotlines in turn contact the ISP to look at it. No company argues with the hotlines and questions their decisions. If the ISPs do not act expeditiously they are liable and can be sanctioned. Hotlines in Britain are supported by the industry and represent a genuine self-regulatory mechanism. Factually they do not consider any type of content and P2P and email messages are excluded from their scope as private communication.

In the course of the following debate the notice and take down procedure was critically assessed as not always being sufficiently effective and efficient.

The French experience in the removal of source in cases of illegal content on the Internet was presented by **Carole Gay, Legal and Regulatory Affairs Counsel** and **Nicolas D'Arcy, Content Analyst and Lawyer, AFA**. They provided also special information concerning the operation of the French hotline. The French hotline was established in 1998. It reacts on the basis of reports from the public. In every case the allegedly illegal content is subject to the examination of an analyst. The hotline notifies ISPs in France and then ISPs in the US in 48 hours. It works in close cooperation with the French police. Other partners are hotlines abroad and the INHOPE network. In practice the French hotline relies on the database collected by INHOPE. The activities of the hotline are made known to the public through various communications tools mainly leaflets and regular press releases.

Further in the panel **Jean-Christophe Le Toquin, Microsoft** described one of the innovative strategies of the company – the photo DNA technology with which 20 million images per day can be analyzed.

Adrian Dwyer, Executive Director of INHOPE expanded on the issue about the role of the hotlines dwelling particularly on the contribution of the INHOPE network to the prevention of child abuse. INHOPE comprises hotlines in 35 countries and its task is to assist them in the removal of images of child pornography. It has at its disposal a unique dataset. An interesting project supported by INHOPE is the establishment of a charitable foundation to help set up hotlines in the developing countries. It aims at identifying possible partners in these countries and provides training and support for institutions and organizations there.

At the end of the session **Regina Jensdottir, Head of Children's Rights Division at the Council of Europe** spoke about the "One in Five" campaign of the Council of Europe aiming at preventing children from sexual violence on the Internet through active awareness raising and promotion of friendly and trusted environment. The name reminds of the worrying statistics showing that every one of five children is exposed to sexual abuse on line. Launched in November 2010 the campaign pursues a number of highly relevant goals – to encourage the signing and ratification of the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, to promote the Council of Europe guidelines concerning the creation of communications environment of justice and trust, to equip children with the necessary tools against sexual violence by developing child friendly materials. The One in Five campaign works together with a network of 43 PACE members who bring the ideas of the campaign back to their countries and work on the ground for the accomplishment of its noble goals. Other partners are the UN special representative and the UNICEF regional Office.

In the debates the CDMC representative drew attention to some of the instruments prepared

Министерство на транспорта, информационните технологии и съобщенията на Република България 2014 Всички права запазени
Министерство на транспорта, информационните технологии и съобщенията

by the committee more precisely the recommendation on measures to protect children against harmful content and behaviour and to promote their active participation in the new information and communications environment and the declaration on protecting the dignity, security and privacy of children on the Internet. The point that a follow up to the declaration concerning the removal or deletion of content as well as its traces which can jeopardize the future of children and render them vulnerable at later stages of their life has to be considered by member states and other stakeholders with the view of taking action in this direction was particularly stressed.

The workshop on the prevention of child abuse in cyberspace covered a broad range of issues spanning legal, institutional and technological questions. The general conclusion of the discussions was that the problem of child abuse is a societal problem that requires joined efforts of state bodies, private sector and non-governmental organizations. A complex of measures can be implemented but they have to be properly ensured. Prevention, protection and prosecution are different stages of a whole process that mutually reinforce each other.

The final plenary session of the Octopus conference was dedicated to two crucial themes - the protection of human rights in cyberspace and the future cooperation against cybercrime.

From the presentation of **Rachael Kondak** from **the European Court of Human Rights** it became clear that the case-law of the Court is relevant to the conditions and safeguards limiting investigative powers in cases of crimes on the net. With regard to the human rights that deserve special attention and protection when there is conflict of rights in cyberspace art. 8, art.10 and art.17 ECHR were explicitly pinpointed. Judgments of the Court related to Internet are limited; however, the general principles of the ECHR developed and enriched in the jurisprudence of the Court and applicable to off-line environment are still valid in the on-line environment. In the same vein several other observations merit particular attention. First, it is the importance of the principle of proportionality which is a major tool for reconciling conflicting rights and should be consistently applied to cases in cyber space. Second, it is necessary laws to keep up with technology and to reflect the changes in the complex multidimensional reality. Third, member states have to realize and implement their positive obligation to combat violence and any unlawful act on the Internet by using criminal measures creating at the same time effective system of guarantees.

Does the Cybercrime Convention itself establish an adequate system of guarantees for human rights that might be infringed when its provisions are put into practice? **Prof. Henrik Kaspersen, the Netherlands** who is one of the founding fathers of the convention provided the answer. Getting back to the process of elaboration of the instrument he stressed the fact that the intention of the creators was to harmonize the substantive and the procedural law while leaving aside investigative powers. The presumption was that when investigative powers were applied member states had to be ready to ensure the protection of human rights under their domestic legislation. In practical terms this means that parties to the convention should have a legal system devised on the basis of the principles of human rights. More specifically they should have at their disposal an effective mechanism of protection of the rights including clear and transparent investigative procedure taking into account the equality of arms of prosecution and defense and the necessity of balancing of conflicting rights.

The US perspective on the issue of rights was given by **Joseph Schwerha (USA)** who spoke about the American constitutional protection of rights. Dwelling particularly on the procedures for obtaining digital evidence Mr. Schwerha explained that they were triggered under a complex combination of state and federal laws. Comparing the ECHR and the US approach to evaluating evidence he discussed the principle of proportionality and how it could be perceived within the American legal context. According to him this principle could possibly be construed and applied as a principle of getting the most precious data in the procedure and of proving that this data is relevant for the final decision.

The end of the Octopus conference was marked by a vigorous debate on the future of the international cooperation against cybercrime. Speakers and audience were all united by the opinion that cybercrime is a common enemy and the fight against it should be carried out by

Министерство на транспорта, информационните технологии и съобщенията на Република България 2014 Всички права запазени
Министерство на транспорта, информационните технологии и съобщенията

common means. This global task needs a strong and unconditional message expressing the determination of the international community to be sent to the organized crime. A signal for it is the successful accomplishment of international operations to dismantle organized criminal activity. Examples of such effective operations and of good police practices should be available on the Internet and should be widely promoted.

Considering the situation in various states most of the participants agreed that the developing countries have much less international cooperation instruments at their disposal due to inadequate resources. Collaboration in the field poses challenges for these countries which in practice means vulnerability and insecurity of a significant number of Internet users. Against such a background comprehensive cooperation involving other organizations – OSCE, OECD, ITU – is vital and should continue pursuing a realistic workable strategy. The latter should be based on the principles of democratic political development, economic growth and diminution of the digital gap. Within such a framework much energy and funds should be deployed in the elaboration of new legislation, in the improvement of law enforcement mechanisms and in capacity building. In more concrete terms steps should be undertaken for supplying law enforcement authorities with suitable tools for action and for better professional training of the judiciary.

A comprehensive strategy cannot be successfully put in practice if there is no mutual trust among the different stakeholders. Communication and exchange of operational information with the private sector comprises an unalienable part of such an approach. Another pillar is the involvement of civil society which calls for constant interaction with the public and responding to its demands and interests.

An important segment of the comprehensive strategy is the organization of conferences pursuing specific ends and turning their conclusions and recommendations into concrete actions supported by the necessary resources.

In the course of the debates skeptical voices were raised concerning the availability of the resources needed for all types of initiatives proposed. In a time of crisis such critical views prove more pertinent than ever. Some of the experts suggested possible solutions. Sustainable funding can be secured provided countries work together and cut costs (connected to this proposal is the inference that multiple jurisdiction should be avoided); business can also contribute to financing; regional training centres and centres of excellence with specialized units can be established and the opportunities of the new technologies should be exploited creatively by organizing training and seminars on-line as well as video-conferences.

The general conclusions of the conference are accessible on-line at (http://www.coe.int/t/DGHL/cooperation/economiccrime/cybercrime/cy_Octopus_Interface_2011/2079IF11_conclusions_V7_30nov.pdf), however, I would like to summarize my impressions from the discussions of the Octopus conference 2011 by the following sentence: Cybercrime and cybersecurity are interrelated in the modern complex world, the higher the effectiveness of the fight against cybercrime, the higher protection Internet users will enjoy, cybercrime and cybersecurity strategies are complementary and their implementation can lead to positive results for all citizens if based on commonly cherished values – human rights, democracy and rule of law.

No doubt the highlight of the whole event was the special meeting organized to celebrate the **10th anniversary of the Cybercrime (Budapest) convention**.

In a nut shell the story of the elaboration of the Cybercrime convention goes as follows:"The Cybercrime Convention was signed on 23/11/2001 in Budapest. Open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration, in Budapest, on 23 November 2001. Conditions for entry into force: 5 Ratifications including at least 3 member states o the Council of Europe.

Министерство на транспорта, информационните технологии и съобщенията на Република България 2014 Всички права запазени
Министерство на транспорта, информационните технологии и съобщенията

Entry into force : 1 July 2004."

According to the Explanatory Report "the Convention is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception.

Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation.

The Convention is the product of four years of work by Council of Europe experts, but also by the United States, Canada, Japan and other countries which are not members of the Organisation. It has been supplemented by an Additional Protocol making any publication of racist and xenophobic propaganda via computer networks a criminal offence."

The special meeting to mark the 10th anniversary presented an opportunity the global role of the convention during the years to be publicly praised and proposals for its future implementation to be put forward. Officials of high rank both at the level of the Council and at the level of the states (ministers, attorney generals, solicitor generals, public prosecutors) attended this not only engaging but also exciting session. Discussions were opened by **Mr. Thorbjorn Jagland, Secretary General of the Council of Europe** and closed by **Ms.Maud de Boer-Buquicchio, Deputy Secretary General of the Council of Europe** who expressed their approval of the global impact and effectiveness of the instrument. As Mr. Jagland pointed out it is a genuine global mechanism by creation and operation - Canada, Japan, South Africa and the USA participated in the convention's preparations and most recently Argentina, Australia and Senegal have been invited to join. So far, 55 countries have ratified or signed or been invited to accede to it which comprises an impressive international achievement. Representatives of different countries – parties and potential parties to the convention – the "founding fathers" and international experts took the floor to express their appreciation and support for the outcomes so far. The prevailing general opinion during the session was that due to the principles espoused by the convention international cooperation against criminal acts in cyberspace was strengthened and it had helped business and individuals to benefit from the new information and communications technologies. While 10 years ago the Cybercrime convention was a visionary instrument, nowadays it is an effective tool to ensure safety on the Internet. As an enforcement mechanism it relies on three important pillars – definition of offences, procedural law regulation and way for prevention, detection and investigation of crime. The Budapest convention has enormous potential and remarkable contribution on a global scale. All these features allowed President Obama to include it as a core element in his Internet strategy.

Though quite often we speak about legal instruments as static tools which cannot well keep pace with developments in society the Budapest convention has proved through time that it is a living organism that can stand technological and legal challenges. It has been and will be used to settle newly emerging problems. Following this line it was supplemented by the protocol of racist and xenophobic speech disseminated via computer systems. At present an important issue is cloud computing which raises both jurisdictional and investigative problems and needs careful examination. If new protocols to the Budapest convention are necessary new parties will be involved in the drafting, a fact that will reinforce its global nature.

Министерство на транспорта, информационните технологии и съобщенията на Република България 2014 Всички права запазени
Министерство на транспорта, информационните технологии и съобщенията

In this meeting the **industry** once again voiced its support for the Council of Europe Convention on Cybercrime. In his intervention the representative of Microsoft emphasized that the company had consistently collaborated with the Council of Europe for the accomplishment of safe and secure Internet environment. He also declared that the private sector was committed to assist governments in their efforts to combat cybercrime. There are three important objectives which stakeholders should pursue – to enhance international collaboration, to continue the fight against computer crimes as an international project and to discuss how to sustain funding.

Cooperation, assistance, capacity building – these were **key concepts** underpinning the bright future of the convention. **The Minister of the Judiciary** of **Senegal** spoke on behalf of Africa which strives to be the leader in the field of cybercrime prevention and protection. A central point in his intervention was the digital divide between affluent and poor countries. What Africa needs most today in order to combat effectively cybercrime and to cope with the challenges of the new information and communications environment is technical assistence. The Global Project is the proper platform that could provide adequate training and technical support for the attainment of this highly relevant goal.

In a video address **Mr. Reinhard Priebe, Director of Internal Security, DG Home, European Union**, expressed the position of the EU on the occasion of the anniversary. He acknowledged the Budapest convention as the first international treaty setting a global framework for harmonizing legislation against cybercrime and promoting international cooperation. Further he said that the fight against cybercrime is a priority for the EU but it remained sceptical about the drafting of a new international instrument in the field. He appealed to the nine EU member states which had not ratified the convention so far to do this without delay offering the support of the EC to speed up the process. After briefly outlining the work of the EU for fostering cooperation and capacity building in order for states could prepare their national legislation to join the Budapest convention Mr. Priebe confirmed the excellent cooperation existing between the EU and the Council of Europe in this particular area (as in many others) counting on complementarity and avoiding duplication.

The conclusion of the special meeting was that by implementing the Budapest convention a remarkable bulk of work had been done aiming to create a safe and friendly Internet environment around the globe. However, additional efforts were needed to settle the newly emerging problems and to preserve and enhance the achievements of this unique Council of Europe instrument.

It was only logical that after the active exchange of viewpoints and proposals during the conference and the recap of the work done so far during the celebration meeting the Cybercrime Convention Committee (T-CY) would hold its plenary meeting. The Cybercrime Convention Committee of the Council of Europe is responsible for following the implementation of the Budapest convention. During the meeting a number of important issues concerning on the one hand, the expansion of the convention and the settlement of the most topical contemporary problems in the field, on the other were laid on the table. The committee analyzed the proceedings of the Octopus forum and the proposals made there in order to structure its programme for the future in the best possible way.

It was announced that the number of ratifications, signatures and accessions to the Budapest convention and the additional protocol against racism and xenophobia on the net was rapidly increasing. Several countries are in an advanced stage of the process of accession. Among them Austria is intending to ratify the convention very soon, Turkey will do this next year, in the Dominican Republic changes in domestic legislation including the constitution are underway which will enable the legal system to be prepared for the ratification, the Philippines are very close to passing a law on cybercrime through which the preparations for accession will be completed, in Lichtenstein the ratification instrument will be sent to the parliament in the first half of 2012. The Check Republic, Canada and Japan have also undertaken steps towards becoming parties to the Budapest convention. Finland has ratified the additional protocol on

Министерство на транспорта, информационните технологии и съобщенията на Република България 2014 Всички права запазени
Министерство на транспорта, информационните технологии и съобщенията

xenophobia and hate speech. The protocol has already been ratified by 20 countries, a fact which illustrates the support for the Council of Europe policy against discrimination, racist propaganda and hatred disseminated via the Internet.

What struck everybody present was the great interest in the ratification of the convention demonstrated by many non-European states and their strong commitment to cooperate with the Council of Europe in the struggle against crime in cyberspace. Countries like Senegal, Tonga, Botswana, Sri Lanka, Paraguay and Costa Rica have already voiced their readiness to work together with the state parties for the accomplishment of the objectives of the convention. Their participation and contribution in the global fight against cybercrime is most valuable as it proves the universal validity of the principles of the Budapest convention. One of the items on the work programme of the T-CY mandated the committee to engage in policy dialogue with the different groups of countries, to offer technical assistance if necessary and to support the accession of the largest possible number of states.

The committee devoted part of its time to address the issues of jurisdiction and transborder access to data and data flows which were frequently referred to during the days of the conference. Under the advent of the new information and communications technologies increasingly data is stored on computer systems in locations and jurisdictions other than the physical location of the suspect or his/her computer. Often it happens that the precise location of the data stored in the cloud is unknown to the investigation team and even to the user. The evolution towards cloud computing may become an obstacle for the rapid execution of the investigatory procedures, more precisely the securing of electronic evidence, the pursuing and the prosecuting of the offender. In such situations the right to privacy, data protection and other fundamental rights should be ensured and a balanced and proportional solution should be found in order for human rights and criminal justice to be reconciled. In transborder operations which cut across different jurisdictions it is crucial to formulate clearer rules what is and what is not allowed in each jurisdiction and how states can effectively cooperate among themselves. Such an exercise touches upon the human rights and the rule of law justification of the fight against cybercrime.

In order to cope with these complex issues the Cybercrime Convention Committee decided to set up an ad-hoc group which after considering the matter would be able to come up with a decision either for amending the convention or for drafting an additional protocol or a recommendation with the purpose of regulating properly the transborder access to data and data flows as well as the use of transborder investigative measures on the Internet and other related problems.

Another topic on the agenda regarded the facilitation of the accession to the convention by non-member states, on the one hand and the strengthening of the transparency and predictability of the process, on the other. The Cybercrime Convention Committee (T-CY) has prepared an opinion on the changes in the accession criteria and procedure under art.37 of the Convention. There it is highlighted that "the broadest possible implementation of the Budapest convention, including accession by non-member states, will serve the aim of effective international cooperation against cybercrime."

The central task of the committee in this respect will be to provide the Committee of Ministers and the Parties to the Convention with a technical assessment by cybercrime experts regarding the ability of the applicant non-member states to fully cooperate with the other parties for the accomplishment of its aims. Preparedness however, means not only technical equipment but legislative reforms and institution building in the country invited to join. An important criterion for accession is that effective procedural guarantees providing for the adequate protection of human rights and liberties as stipulated by art.15 of the Convention are in place. The unswerving support for the values espoused and the firm commitment to cooperate to the widest extent possible comprise benchmarks which the applicant state should meet. Indicators for this may include the existence of an efficient administrative infrastructure, the availability of trained staff, existence of record of cooperation relevant for the fight against cybercrime,

Министерство на транспорта, информационните технологии и съобщенията на Република България 2014 Всички права запазени
Министерство на транспорта, информационните технологии и съобщенията

receipt of technical assistance from the Council of Europe, etc.

The procedure of assessment and accession should be just and transparent based on the official communication between the non-member state willing to adhere and the competent Council of Europe bodies without informal consultations.

During its plenary meeting the Cybercrime Convention Committee adopted also its plan for the period 1 January 2012 – 31 December 2013. The realization of the plan titled "The Way Forward" envisages the enlargement of the Budapest convention on a global scale which to a large extent depends on the efforts of the parties to the Convention and the Committee itself. That is why the latter should be independent and creative in its operation. The involvement of new countries performing various roles as parties, signatories and partners and the establishment of relationships of different scope requires the preparation of well thought time-frames for the successful accomplishment of objectives pursued. The new dynamic situation demands also a pro-active role on the part of the Committee and efficient use of resources. There are priorities which is necessary to be clearly outlined as for instance, the support for the acceleration of the process of ratification and accession to the Convention, the review of the effective implementation of the instrument, the possible amendments and supplements to the Convention either through changes in the text, protocols or adoption of "soft law" acts, active international cooperation and coordination in the field, exchange of information and good practice examples, collection of evidence in electronic form, etc. The work plan included all these tasks providing a sound basis for future activities.

Notwithstanding the increase of threats and attacks over computer systems day by day the achievements of the Budapest convention and its growing popularity provide grounds for optimism. The ten years of implementation of the convention have brought forth a range of measures and partnerships against cybercrime. Prevention represents an important stage in the fight against attacks in cyberspace. It is a broad category encompassing the elaboration of standards as well as practical steps such as: constant provision of information about the opportunities and the risks of Internet; formation of special skills and behaviour of users and especially of young people; distribution of materials; organization of campaigns; promotion of good models and practices, etc. Freedom of expression and the media are crucial tools for attaining these goals in the modern world. The Octopus conference was an interesting and lively forum where various issues concerning cooperation and security on the net were discussed, however, the criminal law solutions prevailed. References to other rights particularly to freedom of expression and freedom of the media which may be put at stake while implementing criminal legal measures or the potential of which can be used when combating cybercrime were rare. It could be recommended the interdisciplinary work of the Steering Committee on the Media and Information Society which is going to succeed the Steering Committee on the Media and the New Communication Services to be regularly and comprehensively presented at the Octopus conferences. Areas of cross-sectoral efforts where the expert knowledge of both CDMSI and T-CY could be applied are also worth being identified.

Министерство на транспорта, информационните технологии и съобщенията на Република България 2014 Всички права запазени
Министерство на транспорта, информационните технологии и съобщенията

Министерство на транспорта, информационните технологии и съобщенията на Република България 2014 Всички права запазени