

Presidency conclusions of the Cybercrime Conference which took place on the 12-13th of April 2011, Budapest

“Budapest Conclusions “

On 12th and 13th of April 2011 the Hungarian Presidency hosted a Cybercrime Conference in Budapest which was attended by representatives of the EU Member States, the European Commission, Europol and experts from the US as well as non governmental and private sector participants. On the basis of the discussion and presentations the Hungarian Presidency has drafted the following conclusions.

The free movement of persons is one of the most fundamental freedoms within the European Union. To enforce this right Member States are working together to establish a common, border-less European area of freedom, security and justice, which also guarantees the appropriate level of safety for persons.

While working towards this goal we tend to forget that we already have a border-less area ensuring free movement globally: cyberspace.

In order to guarantee an appropriate level of protection in the area of freedom, security and justice, we should create a common secure European cyberspace as well. This however requires more advanced strategic and operational cooperation than currently exists between the competent entities at national, European and international level.

The European Union with its advanced and continuously evolving internet infrastructure is a popular target of cybercrime. Effective action against cybercrime requires a comprehensive and horizontal approach. It is a global area, where the factors supporting the mobility are given.

Cybercrime, in and of itself, causes considerable damage, however increasing attention should be devoted to the examination of the link between cybercrime and other forms of organized crime. Crimes committed with or against computer tools can result in significant gains, which may be used by criminals for committing further types of organized crime. The global presence of organized crime, supported by the internet and involving significant amounts of data poses a real challenge for our law-enforcement bodies tasked with processing such high volumes of information given the limitations of currently available resources.

Improving efficiency in the fight against organized crime is a priority for the Hungarian Presidency. The Stockholm Program as well as the Internal Security Strategy emphasises some typical categories of organized crime, where European cooperation in tackling the problem is essential. The fight against cybercrime is one of these categories.

We should use existing information from previous findings on this issue and we must also identify further opportunities to improve cooperation in our approach to tackling

cybercrime. To this end, the Hungarian Presidency has organized a conference on the 10th anniversary of the signature of the Budapest Convention concerning the issue of the fight against cybercrime. On the first day of this conference we held an expert level discussion about the possibilities for more effective cooperation between the different law-enforcement bodies, and between law-enforcement and non-governmental organisations and representatives of the private sector in the context of addressing cybercrime.

Considering cybercrime's unique nature, faster exchange of information, better resources for prevention and better level of preparedness of all concerned parties is necessary for effective actions against infringements and/or crimes at national, European and international level.

Furthermore, we need a new strategic and operational cooperation at European level, the outcome of which should be reflected in the next long-term financial program of the European Union, including the establishment of the European Centre against Cybercrime, the creation of a European forum and therefore an active partnership between the police as well as the related authorities along with the development of prevention and awareness-rising.

Referring to the Council Conclusions on the 10th of April 2010, in which the Council stated that the establishment of a European Centre against Cybercrime would be a significant step, we urge the establishment of this Centre as soon as possible, considering the already available resources, in order that the Centre becomes an efficient actor for the coordination of the collection, analysis and exchange of information, for the contact between the relevant authorities of the Member States, and for the creation of partnership between non-law-enforcement agencies as well as concerned entities of the private sector.

Taking into account, we have further possibilities in the field of training the police personnel; we should build upon the capacities of the CEPOL, and ensure that training programmes support primarily the efficiency of the operational work.

Considering, that faster exchange of information implies a closer strategic and operational cooperation, we proposed the creation of a European-wide forum – building upon Europol's already available technical capabilities – for all the actors involved in fight against cybercrime and therefore provide the possibility of real-time information exchange. There is no need to set up a new database instead we should ensure that all participants can reach the key information at the shortest possible time therefore enabling the fastest local reaction.

Since the law-enforcement agencies do not necessarily have the latest information, in the spirit of mutual trust and with the appropriate safeguards and limits, the non-law-enforcement agencies and involved parts of the private sector should also be able to join to the forum for sharing information for our mutual benefit.

Based on the nature of the forum, we have to make it possible for all joining actors to indicate the emerging problematic cases, including the sharing of the domain names.

The prevention, raising social awareness and the involvement of the public into the fight against cybercrime has significant added-value for all actors, and the training of citizens and internet users is one of these possibilities. The governmental, the non-

governmental and the private sector have to undertake this together. The development and the identification of really effective methods for attracting the attention of target groups also needs further examination through different studies concerning this field.

We shall encourage all computer, software and telecommunication companies and suppliers, – whether by means of internet access providing services – to install software providing easily activated awareness-raising and security options in advance; self healing for instance.

We shall further support law enforcement efforts to make internet governance bodies tackle abuse of critical Internet resources more effectively. Moreover, code of conducts concerning the take-down of illegal online content might be considered in cases where industry partners fail to protect users.

Cybercrime is furthermore linked to the sexual exploitation and abuse of children and thus threatens the most vulnerable members of our societies. We welcome the standards, tools and good practices deployed by the European Union, the Council of Europe and their respective Member States but also by civil society and the private sector aimed at the protection and empowerment of children. We call on all stakeholders to make best possible use of these and to cooperate with each other in the development of the future measures.

Paying special attention to legal considerations, we note that the Budapest Convention of Council of Europe on Cybercrime, in the ten years since it was opened for signature in 2001, has achieved worldwide impact. It serves as the legal framework of reference for fighting cybercrime at global level and as a catalyst for capacity building, training and public-private cooperation.

We, therefore, reiterate the statement already made in the Stockholm Programme of the European Union that Member States of the European Union should ratify the Budapest Convention of Council of Europe as soon as possible. The European Union, the Council of Europe, the USA (as a party to this treaty) and other signatories and partners should support the implementation of this Convention in all regions of the world through technical assistance, policy dialogue and other means.

Harmonised legislation in line with the Budapest Convention of Council of Europe, stronger criminal justice capacities and a larger number of Parties to this treaty will greatly enhance efficient international cooperation across jurisdictions.

Considered as a Presidency priority, we spare no effort to update the Union's legislative framework on cybercrime and look forward to finalising negotiations on a Directive in the Council by June this year

We must build upon the exchange of experiences and best practices as well as on suitable capabilities for monitoring and persecute, including the European level implementation of the results of the joint working group of the European Union and the United States for combating against cybercrime. We regard the dialogue between the European Union and the United States as a good example of international cooperation.

13. April 2011. Budapest