ΚΥΠΡΙΑΚΗ ΔΗΜΟΚΡΑΤΙΑ
REPUBLIC OF CYPRUS

Informal Meeting of the Justice and Home Affairs Ministers

Nicosia,
23-24 July 2012

DISCUSSION PAPER – SESSION II (23/7/2012)

Tackling Cybercrime at EU Level: Priorities for the Future

Overview

Over the last decade, the Internet is being more broadly used than ever and has become an essential, integral and indispensable tool of every aspect of modern society and economy for the majority of the population in Europe and beyond.

Inevitably, cybercrime has been rising in parallel and has reached alarming proportions. As economies and payment systems become more and more Internet-based, cybercriminals do commit various crimes such as identity and data theft and fraud. Cybercrime has become a significant multi-million sector of the underground economy and is affecting governments, individuals and businesses. Cyber-attacks may endanger critical infrastructures or amount to terrorist attacks. Traditional crimes like fraud, sexual child abuse and industrial espionage can now be committed in or through cyberspace. Moreover, cybercriminals are not bound by national borders, in contrast to law enforcement agencies.

The European Union, because of its advanced (Internet) infrastructures, increasing Internet-based economies and dependency on communications networks and services, is vulnerable to cybercrime and cyber-attacks. Therefore, public authorities must ensure safety and security for their citizens and societies in cyberspace.

The EU has at various occasions recognized and addressed this threat, confirming its willingness for better security measures in order to protect its citizens from organized cybercrime and terrorism:

- The Europol Organised Crime Threat Assessment (OCTA) 2011 identifies cybercrime as a criminal phenomenon which requires high levels of intelligence coordination and analysis in the framework of law enforcement cooperation in order to gain accurate insight and provide targeted responses.

- The European Council in the Stockholm Programme calls upon Member States to give their full support to the national alert platforms in charge of the fight against cybercrime and emphasises the need for cooperation with countries outside the Union, invites the Commission to take measures for enhancing/improving public-private partnerships and calls upon the Member States to improve judicial cooperation in cyber crime cases. To this extent, the European Council also called upon the Union to clarify the rules on jurisdiction and the legal framework applicable to cyberspace within the Union, including how to obtain evidence in order to promote cross-border investigations. .

- Consequently, on 7 June 2012, the Council affirmed its support for the establishment of a European Cybercrime Centre (EC3) and in its conclusions called upon the Commission, in consultation with Europol, to further elaborate the scope of its specific tasks together with more detailed costings in order to estimate the resources that would be required to make the EC3 operational in 2013. It also acknowledged the need to take the EC3 into account in the allocation of resources to Europol.

- The Council, on 7 June 2012, also endorsed the creation of a Global Alliance against Child Sexual Abuse Online.

- Moreover, in the area of prevention and response to digital crime, particularly cyber-attacks, the Council and the European Parliament are currently negotiating on the Directive on Attacks against Information Systems. This Directive was proposed in 2010 and builds on an existing Framework Decision from 2005.

Next steps

However, issues of jurisdiction and differences in the legislative systems remain at national and at European level. In addition, law enforcement and judiciary staff are frequently not adequately trained in this area. Inevitably, there are at national and EU level still a lot of gaps to cover, measures to

improve, acts to be taken and coordination to be improved. The complexity and breadth of the issue implies that many aspects have to be taken into account and many stakeholders to be involved.

Successfully tackling cybercrime requires effective:

- Preventative measures
- Measures to mitigate its impact and respond at technical level
- Enforcement measures, including procedures and tools for the effective investigation of cybercrimes.

It will undoubtedly require better coordination at national and international level between different agencies dealing with cybercrime and identification of the shortcomings in the prevention and fight against cybercrime. In doing so, cooperation mechanisms with the European Cybercrime Centre will need to be established. Member States should also consider removing procedural obstacles to undercover investigations in order to enable prosecution of perpetrators in the "dark areas" of cyberspace, who now all too often escape notice.

Discussion points

Ministers are invited to respond to the following questions:

1. ***Do Member States have a national strategy dealing with cybersecurity and cybercrime and, if so, what are its key features and main successes?***

2. ***What are the three most important challenges in the fight against cybercrime in the coming years?***

3. ***How can the European Union contribute to an effective response to cybercrime?***

The outcome of this reflection is envisaged to constitute a valuable input to the European Strategy on Cyber Security that is currently under joint preparation by the European Commission and the High Representative.