



**COUNCIL OF  
THE EUROPEAN UNION**

**Brussels, 4 April 2012**

**8295/12**

**LIMITE**

**ENFOPOL 87  
TELECOM 71**

**NOTE**

---

From: Presidency  
To: Law Enforcement Working Party  
Subject: Draft Council conclusions on the establishment of a European Cybercrime Centre

---

Following the publication of the Commission Communication "Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre" delegations will find enclosed the proposal from the Presidency for draft Council Conclusions on the establishment of a European Cybercrime Centre to be discussed at the LEWP meeting on 13 April 2012.

**Draft Council conclusions**  
**on the establishment of a European Cybercrime Centre**

THE COUNCIL OF THE EUROPEAN UNION

HAVING REGARD to the fact that the Internet has become an integral and indispensable part of modern society and a facilitator of economy growth in the EU;

MINDFUL of the increasing threats to Union citizens and businesses posed by cybercrime;

AWARE that the European Union, in particular, is a key target for cybercrime because of its advanced Internet infrastructure, its high number of Internet users and its increasingly Internet-based economies and payment systems;

CONSCIOUS that no other type of crime is as transnational in nature as cybercrime and that cybercrime often affects a large number of victims and involves suspects in many different parts of the world;

AWARE that wide-scale cross-border cybercrime operations cannot be successfully conducted by national police forces alone, but require that law enforcement authorities adopt a coordinated and collaborative approach together with public and private stakeholders;

RECALLING the Council of Europe Convention on Cybercrime of 23 November 2001 that calls for international cooperation to protect society from this phenomenon;

RECALLING that the European Council in the Stockholm Programme invited the Commission, inter alia, to take measures to enhance/improve public-private partnerships in the field of fighting cybercrime, invited Europol to step up strategic analysis on cybercrime and invited Member States to improve judicial cooperation in cybercrime cases;

RECALLING that the Council has made the fight against cybercrime and the criminal misuse of the Internet by organised crime groups one of the European Union's priorities in the fight against organised crime between 2011 and 2013<sup>1</sup> within the framework of the EU Policy Cycle for organised and serious international crime;

NOTING that one of the strategic goals<sup>2</sup> related to this Union's crime priority is the establishment of the European Cybercrime Centre as a focal point in the fight against cybercrime in the Union, contributing to faster reactions in the event of cyber attacks;

RECALLING the Council conclusions on a Concerted Work Strategy and Practical Measures Against Cybercrime<sup>3</sup>, inviting Member States and the Commission to introduce measures based on case studies, particularly taking into account technological developments, so as to prepare tools for operational use in the short and medium term;

BUILDING UPON the Council conclusions on an Action Plan to implement the concerted strategy to combat cybercrime adopted on 26 April 2010<sup>4</sup>, in which the Council invites the Commission to draw up a feasibility study on the possibility of creating a Cybercrime Centre to fulfil a number of tasks in the fight against cybercrime;

---

<sup>1</sup> 11050/11 JAI 396 COSI 46 ENFOPOL 184 CRIMORG 81 ENFOCUSTOM 52 PESC 718 RELEX 603.

<sup>2</sup> 15850/11 JAI 758 COSI 84 ENFOPOL 371 CRIMORG 191 ENFOCUSTOM 128 CORDROGUE 67 PESC 1321 RELEX 1081 COAFR 296 COWEB 236 TRANS 283 UD 275 FRONT 138 GENVAL 111.

<sup>3</sup> 15569/08 ENFOPOL 224 CRIMORG 190.

<sup>4</sup> 5957/2/10 CRIMORG 22 ENFOPOL 32.

NOTING that Article 4 of the Council Decision of 6 April 2009 establishing the European Police Office (Europol)<sup>5</sup> has, in conjunction with the Annex to that Decision, conferred on that agency the competence to cover computer crime;

CONSIDERING also that the Europol Organised Crime Threat Assessment (OCTA) 2011 identifies cybercrime as a criminal phenomenon which cannot be combated effectively by law enforcement alone but requires high levels of central intelligence coordination and analysis in order to gain accurate insight and provide targeted responses;

CONSCIOUS that although the Union has developed various initiatives to tackle cybercrime, several obstacles still remain at European level to the effective investigation of cybercrime and prosecution of offenders;

## **HEREBY**

WELCOMES the Commission's Communication "Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre"<sup>6</sup>, proposing to set up a European Cybercrime Centre through which Member States and EU institutions will be able to build operational and analytical capacity for investigations and cooperation with international partners;

AGREES that the European Cybercrime Centre should, in particular, focus on cybercrime committed by organised crime groups, cybercrime which cause serious harm to their victims, and cybercrime affecting critical infrastructure and information systems in the Union while ensuring the necessary flexibility to react to the emergence of new cybercrime threats;

CONFIRMS that the European Cybercrime Centre should serve as the European cybercrime information focal point; that it should pool cybercrime expertise to support Member States in capacity building; that it should provide support to cybercrime investigations in the Member States and that it should become the collective voice of European cybercrime investigators within law enforcement and the judiciary;

---

<sup>5</sup> OJ L 121, 15.5.2009, p. 37.

<sup>6</sup> 8543/12 ENFOPOL 94 TELECOM 72.

SUPPORTS the proposal of the Commission to locate the European Cybercrime Centre at Europol;

EMPHASISES the importance of ensuring close cooperation of the European Cybercrime Centre with other relevant agencies and actors such as Eurojust, CEPOL, Interpol, ENISA, the wider computer emergency response team (CERT) community and not least the private sector, to broaden in practice the information picture on cybercrime in Europe;

UNDERLINES the need for Member States to involve and make use of the European Cybercrime Centre in all cross-border cybercrime operations and investigations;

CONSIDERS that the feasibility study on a European Cybercrime Centre constitutes a good basis for a preliminary estimation of the immediate resource needs for the implementation phase of the Centre;

ACKNOWLEDGES that, whilst resource implications need to be further assessed, the means required to implement the European Cybercrime Centre should be taken into consideration when negotiating the future Europol budget.

---