COUNCIL OF THE EUROPEAN UNION

Brussels, 4 April 2012

8543/12

ENFOPOL 94
TELECOM 72

COVER NOTE

from:	Secretary-General of the European Commission, signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt:	30 March 2012
to:	Mr Uwe CORSEPIUS, Secretary-General of the Council of the European Union
No Cion doc.:	COM(2012) 140 final
Subject:	COMMUNICATION FROM THE COMMISSION TO THE COUNCIL AND EUROPEAN PARLIAMENT Tackling crime in our Digital Age: Establishing a European Cybercrime Centre

Delegations will find attached Commission document COM(2012) 140 final.

Encl.: COM(2012) 140 final

EUROPEAN COMMISSION

Brussels, 28.3.2012
COM(2012) 140 final

COMMUNICATION FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT

Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre

COMMUNICATION FROM THE COMMISSION TO THE COUNCIL AND THE EUROPEAN PARLIAMENT

Tackling Crime in our Digital Age: Establishing a European Cybercrime Centre

1. INTRODUCTION: THE EUROPEAN RESPONSE TO A BORDERLESS CRIME

The Internet has become an integral and indispensable part of our society and economy. Eighty percent of young Europeans connect with each other and the world through online social networks[1], and approximately USD $8 trillion changes hands globally each year in e-commerce[2]. But as more and more of our everyday lives and business transactions happen online, so too does criminal activity - more than one million people worldwide become victims of cybercrime every day[3]. Online criminal activity ranges from selling stolen credit cards for as little as one euro, to identity-theft and child sexual abuse, to serious cyber attacks against institutions and infrastructure.

The total cost of cybercrime to society is significant. A recent report suggests that victims lose around USD $ 388billion each year worldwide as a result of cybercrime, making it more profitable than the global trade in marijuana, cocaine and heroin combined[4]. Although such information should be treated with caution, as different ways of defining what cybercrime entails might lead to varying cost estimates, there is, however, agreement that cybercrime is a high-profit, low-risk form of criminal activity which is becoming increasingly common and damaging. In a time when fostering economic growth is paramount, stepping up the fight against cybercrime will be essential to maintain citizens' and businesses' confidence in secure online communication and trade. It will also support the growth targets set by the Europe 2020 strategy[5] and the Digital Agenda for Europe[6].

The freedom of the Internet is the key factor in explaining the digital revolution of recent years. Our open Internet knows neither national boundaries nor a single global governance structure. But while promoting and protecting this online freedom in line with the Charter of Fundamental Rights of the EU, we must also strive to protect citizens from the organised criminal gangs who seek to exploit such openness. No crime is as borderless as cybercrime, requiring law enforcement authorities to adopt a coordinated and collaborative approach across national borders, together with public and private stakeholders alike. It is here that the EU can, and does, add significant value.

The European Union has developed various initiatives to tackle cybercrime. These include the 2011 Directive on combating the sexual exploitation of children online and child

---

1 Eurostat, Internet Access and Use, 14 December 2010.

2 McKinsey Global Institute, Internet Matters: the Net's sweeping impact on growth, jobs and prosperity. Report May 2011 accessed on 8 February 2012 (.

3 Norton Cybercrime Report 2011, Symantec, 7 September 2011, accessed on 6 January 2012 .

4 Ibid.

5 Europe 2020 – A strategy for smart, sustainable and inclusive growth, COM(2010) 2020, 3 March 2010.

6 A Digital Agenda for Europe, COM(2010) 245 final, 26 August 2010.

pornography, and a Directive on attacks against information systems, focusing on penalising the exploitation of cybercrime tools, especially botnets[7], which should be adopted in 2012. Europol has increased its activities against cybercrime, playing a key role in the recent "Operation Rescue", in which police arrested 184 suspected child sex offenders and identified over 200 victims of child abuse following one of the biggest investigations of its kind by law enforcement agencies across the world. Thanks to the work of Europol analysts in cracking the security features of a key computer server at the centre of the network, the identity and activities of the suspected offenders were uncovered.

The fight against cybercrime, for which the main legal instrument is the Council of Europe Cybercrime Convention[8], continues to be a top priority. It is identified in the EU policy cycle for organised and serious international crime[9], and forms an integral part of efforts to develop an overarching EU strategy to strengthen cyber-security. The EU has also engaged closely with international partners, for example, through the ongoing EU-US working group on cyber-security and cybercrime.

Such progress aside, there are still several obstacles to the effective investigation of cybercrime and prosecution of offenders at European level. These include: jurisdictional boundaries, insufficient intelligence-sharing capabilities, technical difficulties in tracing the origins of cybercrime perpetrators, disparate investigative and forensic capacities, scarcity of trained staff, and inconsistent cooperation with other stakeholders responsible for cyber-security. Through the Instrument for Stability the EU is also addressing the rapidly evolving transnational threats related to cybercrime in developing and transitional countries where the required capacities to fight this form of organised crime are often lacking.

In response to these challenges, the Commission indicated its intention to create a European Cybercrime Centre as a priority of the Internal Security Strategy[10]. Having conducted a feasibility study on the creation of such a centre[11], at the request of the Council[12], the Commission proposes a European Cybercrime Centre (EC3), which will be part of Europol and act as the focal point in the fight against cybercrime in the EU. This Communication drawing on the feasibility study outlines the proposed core functions of the European Cybercrime Centre, explains why it should be located in Europol, and how it can be established. Resource implications will however need to be further assessed and provided for

---

7 Proposal for a Directive of the European Parliament and of the Council on attacks against information systems, COM (2010)517 final, 30 September 2010. Botnets are networks of compromised computers infected by malicious software that can be remotely activated to perform specific actions, including cyber-attacks.

8 Council of Europe Cybercrime Convention, Budapest, 23 November 2001, also known as the Budapest Convention. The Convention is accompanied by an *Additional protocol to the Convention on Cybercrime* concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems.

9 The EU policy cycle for organised and serious international crime, covering the years 2011/2013, has eight priorities, one of which is to "Step up the fight against cybercrime and the criminal misuse of the Internet by organised crime groups".

10 "By 2013, the EU will establish … a 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" in The EU Internal Security Strategy in action: five steps towards a more secure Europe. COM(2010)673 final, 22 November 2010.

11 Feasibility study for a European Cybercrime Centre, Final Report, February 2012.

12 Council Conclusions concerning an Action Plan to implement the concerted strategy to combat cybercrime, 3010th General Affairs Council meeting, Luxembourg, 26 April 2010.

before the EC3 can become fully operational. The establishment of this Centre will be reflected, as appropriate, in the upcoming revision of Europol's legal basis.

2. PROPOSAL FOR SETTING UP A EUROPEAN CYBERCRIME CENTRE

In order for the European Cybercrime Centre (EC3) to provide added value, while respecting the principle of subsidiarity, it is proposed that the EC3 should focus on the following major strands of cybercrime:

(i) Cybercrimes committed by organised crime groups, particularly those generating large criminal profits such as online fraud;

(ii) Cybercrimes which cause serious harm to their victims, such as online child sexual exploitation; and

(iii) Cybercrimes (including cyber-attacks) affecting critical infrastructure and information systems in the Union[13].

Considering the ever-evolving nature of cybercrime, there should also be scope for taking action both in response to Member States' requirements and to deal with the emergence of new cybercrime threats facing the Union.

2.1. Core functions and what a European Cybercrime Centre should deliver

The EC3 should have four core functions:

(a) Serve as the European cybercrime information focal point

A information fusion function would ensure information collection on cybercrime from the widest array of public, private and open sources, enriching available police data. It should gradually bridge current gaps in the information available from the communities responsible for cyber-security and for tackling cybercrime. The information gathered would concern cybercrime activities, methods and suspects. It serves to improve both knowledge of cybercrime and its prevention, detection and prosecution, and to encourage appropriate links between law enforcement authorities, the Computer Emergency Response Team (CERT) community and private sector Information Communication Technology (ICT) security specialists. The sharing of information needs to respect confidentiality agreements and rules between different parties.

The information fusion function would also be useful for improving cybercrime reporting and information sharing. The Commission would like Member States to make it a requirement that serious cybercrime offences be reported to national law enforcement authorities[14]. This would enable national police services to provide information on serious cybercrimes more consistently to the EC3 which, in turn, would disseminate this information so that colleagues in other Member States would know if they are working towards the same target and benefit from each other's information in investigations.

---

[13] As defined in Council Directive 2008/114/EC of 8 December 2008. This Directive is currently under revision, the EC3 would take into account further developments.

[14] Such as the ones listed in Articles 3 to 7 of the tabled draft Directive on attacks against information systems, COM(2010)517 final, 30 September 2010.

The aim is to broaden the information picture on cybercrime in Europe over time so as to produce high-quality strategic reports on trends and threats, to become knowledgeable on the basis of comprehensive crime figures and to improve operational intelligence from an information base which draws on a variety of sources.

(b) Pool European cybercrime expertise to support Members States in capacity building

The EC3 should assist Member States with expertise and training to curb cybercrime. The primary focus is on law enforcement, but training should also be offered to the judiciary. Existing initiatives from Europol, CEPOL and the Member States would be streamlined following a thorough needs analysis in order to ensure better coordination and complementarity. This training should range from in-depth technical expertise to broader capacity building for police officers, prosecutors and judges to tackle cybercrime casework.

A cybercrime desk should be created to exchange best practice and knowledge, and to engage with and respond to queries from Member States and international law enforcement authorities, the judiciary, the private sector and civil society organisations, for example, in the case of cyber attacks or new forms of online scams.

It should support the activities of, and render advice to, cybercrime expert groups, including the European Union Cybercrime Task Force and experts in combating online child sexual exploitation. It should also establish cooperation with the developing network of cybercrime centres of excellence, such as 2Centre, and the research community.

The EC3 should also help Member States in their efforts to develop and deploy an online cybercrime reporting application, based on agreed standards, to link reporting streams from a variety of actors (companies, national/governmental CERTs, citizens etc.) to national law enforcement bodies and from national law enforcement bodies to the EC3.

The EC3 should engage with and facilitate exchange of best practice across the criminal justice community and law enforcement field. Effective involvement of the judiciary in tackling cybercrime is of paramount importance for improving the prosecution of serious cybercriminals across the Member States.

(c) Provide support to Member States' cybercrime investigations

The EC3 should provide operational support to cybercrime investigations, for example, encouraging the establishment of cybercrime Joint Investigations Teams and the exchange of operational information in on-going investigations.

It should also provide high-level forensic assistance (facilities, storage, tools) and encryption expertise for cybercrime investigations.

(d) Become the collective voice of European cybercrime investigators across law enforcement and the judiciary

Over time, the EC3 could act as a rallying point for European cybercrime investigators, providing them with a collective voice in discussions with the ICT industry and other private sector companies as well as with the research community, users' associations and civil society organisations on how to better prevent cybercrime and to coordinate targeted research activities.

The EC3 would be the natural interface to Interpol's cybercrime activities and other international police cybercrime units. It could also coordinate input into ongoing initiatives on Internet governance and the UN's open-ended intergovernmental expert group on cybercrime.

The EC3 should also collaborate with organisations such as INSAFE[15] in the delivery of public awareness campaigns, updating them in response to changes in cybercrime identified by the Centre's analysis with a view to encouraging prudent and safe online behaviour.

2.2. Location

As evidenced in the feasibility study, the European Cybercrime Centre should be part of Europol, located within its existing structures.

This carries distinct advantages. Europol has a recognised role amongst Member States and other stakeholders, including Interpol and international law enforcement authorities, and already has a mandate to deal with computer crime[16]. The core business of Europol is to help achieve a safer Europe for the benefit of all citizens, by supporting EU law enforcement authorities through the exchange and analysis of criminal intelligence.

2.3. EC3 resource implications

The feasibility study has examined different resource implications. These will need to be further assessed[17], notably in the light of other tasks that might have to be carried out by Europol in the future and in the more general context of the staffing of EU Agencies. This assessment will in particular be carried out in the context of the revision of the Europol legal basis and the ongoing discussion on the Commission's proposal for an Internal Security Fund. However, it already appears clear that secondment from Member States will be needed.

When assessing estimated resource needs, the Commission will be guided by three considerations: firstly, it is assumed that there will be a moderate increase in total cybercrime caseload as opposed to a massive rise in cybercrimes; secondly, Member States will enhance their own capability to fight cybercrime; and, thirdly, the EC3 will only deal with a certain set of cybercrimes.

2.4. Governance

Placing the EC3 within Europol would make it important to ensure the participation of other key stakeholders in the strategic direction of the Centre. Therefore, the Commission suggests establishing an EC3 Programme Board within the governance structure of Europol, which would be chaired by the Head of the EC3. This instrument would give other stakeholders, such as Eurojust, CEPOL, Member States, as represented by the EU Cybercrime Taskforce, ENISA and the Commission, the possibility to bring in their respective know-how, without creating unnecessary additional administrative burden. The Board could act to drive accountability for the delivery of EC3 cybercrime activities and thus would ensure that they

---

15 European network of Awareness Centres promoting safe, responsible use of the Internet and mobile devices to young people.

16 Council Decision (2009/371/JHA) of 6 April 2009 establishing the European Police Office, art. 4 (1) in conjunction with annex.

17 The assessment needs to be coherent with the overall staffing and budgetary requirements for agencies in the 2013 Budget and the next Multiannual Financial Framework.

are carried out in partnership, recognising the added expertise and respecting the mandates of all stakeholders.

2.5. Cooperation with key actors

The EC3 should ensure a coordinated response to cybercrime, not only enabling joint working between EU agencies, but also serving as a single European point of contact in this field.

(a) Member States

The key aim is to assist Member States' in the fight against cybercrime. The EC3's cybercrime helpdesk and deliverables, such as more focused threat analysis and better informed operational support will benefit cybercrime investigators across Europe. The EU Cybercrime Taskforce would ensure representation of Member States' concerns on the EC3 Programme Board. Moreover, Member States' will need to continue to make necessary investments in their national structures to fight cybercrime, so as to have adequate interfaces for interaction with the EC3.

(b) European agencies and other actors

Relevant agencies, notably Eurojust, CEPOL and ENISA, as well as the CERT-EU, would be directly involved in the activities of the EC3 not only through their participation in the Programme Board, but also through operational cooperation where relevant and taking into account their respective mandates.

(c) International partners

In its quest to develop into the European cybercrime information focal point, the EC3 should become a valuable interlocutor for international partners on cybercrime matters. The EC3 should, in partnership with Interpol and our strategic partners around the globe, strive to improve coordinated responses in the fight against cybercrime and ensure that law enforcement concerns are taken into account in the further development of cyberspace.

(d) Private sector, research communities and civil society organisations

Building trust and confidence between the private sector and law enforcement authorities is of utmost importance in the fight against cybercrime. Consolidating Europol's work with existing and new partners, the EC3 should build trusted networks and information exchange platforms with industry and other actors such as the research community and civil society organisations. These should facilitate cross-community information sharing on a range of issues, including early warning of cyber threats, and collaborative "task force" style responses to cyber attacks and other types of cybercrime.

The EC3 should also contribute to wider efforts of private sector companies with substantial digital assets, such as banks and online retailers, to fight and better protect against cybercrime and to minimise vulnerabilities in developing technologies.

It is in the mutual interest of law enforcement authorities and the private sector to arrive at a better measurement of the cybercrime landscape in real time as well as to strive for more effective dismantling of cybercrime networks via an enhanced detection of new modi operandi and the swift arrest of cybercriminals.

3. A ROADMAP TOWARDS THE IMPLEMENTATION OF THE EUROPEAN CYBERCRIME CENTRE

3.1. Activities until the end of 2013

In order to reach initial operating capability, the Commission will explore, in close cooperation with Europol, what would be needed in terms of human and financial resources to set up an EC3 implementation team until the end of the current EU financial framework. Tasks of the implementation team would, for example, include drafting of the EC3's terms of reference and its organisational structure, and also development of indicators to assess its performance. The role and functioning of the Programme Board will be further defined and agreed by the associated stakeholders.

With a view to establishing a full information fusion function, the EC3 implementation team should create links to the CERT-EU pre-configuration team, as well as with ENISA where relevant (taking into account their limited resources). To improve cybercrime reporting, a mapping exercise will be conducted to create an interoperability map of existing online cybercrime reporting systems in the Member States.

A cybercrime desk should be established. This desk could be supported by the provision of a dedicated, secure online community platform. Current training activities of Europol, CEPOL and the European Cybercrime Training and Education Group could be assessed and streamlined under the coordination of the EC3 and its Programme Board. A training needs analysis, which also considers requirements of judges and prosecutors, should be conducted. From this review, a basic cybercrime training course, open to members of the criminal justice system, could be delivered.

In addition, a more precise assessment of necessary human and financial resources will have to be made and provided for in decisions under the next Multiannual Financial Framework. This assessment will inform the further development of the EC3.

4. CONCLUSION

As the world of organised crime expands its activities into cyberspace, law enforcement must keep up. The EU can provide Member States and industry with the tools to tackle the modern and ever-evolving menace of cybercrime which, by definition, knows no borders. Provided the necessary human and financial resources can be secured, a European Cybercrime Centre will act as the focal point in Europe's fight against cybercrime; by pooling expertise, supporting criminal investigations and promoting EU-wide solutions, while raising awareness of cybercrime issues across the Union. As such, the Centre would contribute to the safeguarding of an open Internet and the legitimate digital economy, and to the protection of Europe's online citizens and businesses.

The Council is invited to endorse this proposal and the European Parliament as well as other relevant stakeholders are encouraged to contribute to the development of the Centre.