EUROPEAN
COMMISSION

Brussels, 27.3.2013
SWD(2013) 100 final

COMMISSION STAFF WORKING DOCUMENT

Ex-Ante Evaluation:
Resources needed to fulfil the tasks set forth in the Commission's Communication on the establishment of a European Cybercrime Centre (EC3)

{COM(2013) 173 final}
{SWD(2013) 98 final}
{SWD(2013) 99 final}

COMMISSION STAFF WORKING DOCUMENT

Ex-Ante Evaluation:

Resources needed to fulfil the tasks set forth in the Commission's Communication on the establishment of a European Cybercrime Centre (EC3)

1. Introduction

Cybercrime is an increasingly important concern for policy-makers, businesses and citizens. In many countries, societies have come to rely on cyberspace to do business, consume products and services or exchange information with others online.

According to a recent Eurobarometer Survey on Cybersecurity, around half the internet users in the EU say they buy goods or services online (53%), use social networking sites (52%), or do online banking (48%), while 20% sell goods or services.

Modes of connecting are growing ever more complex too. Smartphones can access high-speed data networks, enabling people to surf the internet while on the move, and developments such as cloud computing are helping to realise the possibilities of limitless data storage.

Cyberspace has a downside too. Criminals exploit citizens and organisations to steal money, to commit fraud or for other criminal activities, including identity theft. These can range from a type of fraud called 'phishing' that fools users into revealing passwords or sensitive data, to complex incidents involving breaking into computer networks to steal data such as business secrets or money.

Some misuses aim to destroy information or deny its availability to others, but the motivations behind such attacks may vary from malicious intent, to anger, ideology or political activism. Many cybercrimes target financial institutions or online entities where transactions take place, or revolve around activities that have a direct or indirect physical element of harm against the person — for example, the online exchange of child abuse material. There are crimes that exist only in cyberspace, such as online bullying or stalking via virtual communities.

There is evidence that the phenomenon of cybercrime is growing. A Commission Feasibility Study identified recent data on cybercrime from some EU Member States. These are recorded cybercrime figures, either from the cybercrime units' own management information systems, or from official reports, and thus depend on the particular reporting and recording mechanisms in each country.

Both industry and criminal justice statistics show an increase in cybercrimes. Though neither of these sources provides a robust account of the absolute number of cybercrimes, they can provide an indication of trends over time, on the grounds that in each survey or industry report, data have been (with one or two exceptions) collected in a fairly consistent way over time.

Looking at these data, the phenomenon of cybercrime would appear to be on the rise. However, there is large variance in the range identified and it is not possible to account for what is driving this. Both officially-reported statistics and data provided by industry may provide a skewed perspective. Official criminal justice statistics may under-report cybercrimes due to definition-related reasons, whereas industry figures may over-dramatise the situation, as they need to establish a link between a problem and the solution that might be offered.

The perceptions of EU citizens are, however, also in line with statistics. A July 2012 Eurobarometer Survey found that 74% of EU citizens consider that cybercrime is on the rise and that internet users are very concerned about cyber security: 89% avoid disclosing personal information online, and 74% agree that the risk of becoming a victim of cybercrime has increased in the past year. For those using the internet for online banking or shopping, the two most common concerns are about someone taking or misusing personal data (40% of users) and security of online payments (38% of users).

2. Policy context

The Commission's March 2012 proposal to set up a European Cyber Crime Centre (EC3)was the culmination of a number of policy initiatives in the field of cybercrime that can be traced back to the JHA Council Conclusions in 2008.[1]

In its 2010 **EU Internal Security Strategy** (ISS),[2] the Commission stated that one of the five main objectives was to '**raise levels of security for citizens and businesses in cyberspace**'. The first action necessary to fulfil this objective was to '**Build capacity in law enforcement and the judiciary'.** It went on to state how this ought to be done:

'By 2013, the EU will establish, within existing structures, 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. The centre will improve evaluation and monitoring of existing preventive and investigative measures, support the development of training and awareness-raising for law enforcement and judiciary, establish cooperation with the European Network and Information Security Agency (ENISA) and interface with a network of national/governmental Computer Emergency Response Teams (CERTs). **The cybercrime centre should become the focal point in Europe's fight against cybercrime'.**

The Strategy recognised that 'the High Tech Crime Centre at Europol already plays an important coordinating role for law enforcement, **but further action is needed'.** Subsequently, the European Commission followed up the request of the Council[3] and conducted a Feasibility Study[4] to assess and evaluate the current state of efforts to deal with cybercrime as well as to consider the feasibility of an EC3 across a range of different aspects

[1] JHA Council Conclusions 2899th JHA meeting (2008).

[2] European Commission, COM(2010) 673 final.

[3] Council Conclusions concerning an Action Plan to implement the concerted strategy to combat cybercrime, 3010th General Affairs Council Meeting, Luxembourg, 26 April 2010.

[4] RAND Europe, Feasibility study for a European Cybercrime Centre, Final Report, 2012 .

such as mandate, resources, activities, risks, impact and interoperability with other organisations.

Drawing on the Feasibility Study, the Commission proposed setting up a European Cybercrime Centre 'which will be part of Europol and act as the focal point in the fight against cybercrime in the EU' in its March 2012 Communication to the Council and the European Parliament. The Commission Communication outlined the proposed core functions of the European Cybercrime Centre, explaining why it should be located in Europol, and how it could be established. However, the Commission noted that there would have to be further assessment of the implications for resources, and that these would have to be provided for before the EC3 could become fully operational. It also noted that the establishment of this Centre would be reflected, as appropriate, in the upcoming revision of Europol's legal basis.

On 7-8 June 2012, the Council adopted Conclusions welcoming and supporting the setting up of the EC3. In its Conclusions, the Council also called upon the Commission, 'in consultation with Europol, to further elaborate the scope of the specific tasks of the European Cybercrime Centre together with more detailed costings in order to estimate the resources that would be required to make the Centre operational in 2013, drawing on the feasibility study and the work carried out by the European Cybercrime Centre implementation team. On this basis the Commission shall report to the Council at the Law Enforcement Working Party and, if appropriate, other relevant Council fora, in order to enable the Council to follow up on and support the progress in the setting up and work of the European Cybercrime Centre'.

It is important to assess the role of actors and stakeholders in the cyber sphere, as this influences the work (and thus resources) of the EC3 and vice-versa. It also helps to determine the extent to which a truly comprehensive approach towards tackling cybercrime can be achieved.

Member States' law enforcement authorities have the competence to investigate and prosecute crime. However, the landscape varies in terms of organisation within the national law enforcement system and mandate. Such divergence may hinder effective operational and strategic cooperation at EU level.

At EU level, **Europol** has a mandate to provide criminal intelligence analysis and operational support to Member States to tackle cybercrime. A high-tech crime unit evolved in a rather piecemeal approach since 2001 around three Analysis Work Files (AWFs): on credit-card fraud, child sexual abuse and cyber-attacks. Europol has links with Member States through Europol National Units within the law enforcement authorities (LEAs) of each Member State.

From a judicial/prosecutorial angle, **Eurojust** supports judicial cooperation in cybercrime investigation, for instance, by facilitating coordination and providing advice on legal and regulatory frameworks issues of jurisdiction. **CEPOL** (European Police College) provides EU-wide police training. By developing specialised cybercrime investigation training, it can collate, share and expand the specialised knowledge and expertise law enforcement needs to prosecute cybercrime successfully. The EU Cybercrime Taskforce (**EUCTF),** made up of heads of high-tech crime units of the MS, is another rather loose structure that contributes to work on fighting cybercrime at EU level.

Within MS, national **Computer Emergency Response Teams (CERTs)** are important players in case of an attack on critical IT infrastructure to determine the problem and provide technical solutions to resolve a nation-wide crisis. Their relationships with law enforcement authorities are important to help in investigations and secure prosecutions.

The **European Network and Information Security Agency (ENISA),** established in 2004, has the task of providing support and advice to the Member States, the Commission and the business community in ensuring a high level of network and information security in the Union. ENISA provides an important interface with the CERT community, although it has no powers to address cybercrime operationally. Furthermore, the Commission recently set up its own **CERT-EU** to support the European Institutions in protecting themselves against intentional and malicious attacks that would hamper the integrity of their IT assets and harm the interests of the EU.

In the field of network and information security (NIS), the Commission launched two initiatives in 2009, the **European Forum for the Member States (EFMS)**, a platform for discussion and exchange of best practices among the Member States, and **the European Public-Private Partnership for Resilience (EP3R)**, a platform for discussion and exchange of best practices between the public and the private sector.

The objective of this Ex-Ante Evaluation is to show how setting up the EC3 addresses the problem and what resources are needed to deliver its tasks in the most effective, efficient and coherent way.

Apart from the Feasibility Study, the current assessment takes into account recent developments within Europol and work carried out by the Commission together with the EC3 Implementation Team (set up following the adoption of the Communication to prepare and the launch and roll-out of the EC3)..

3. Problem definition

While the phenomenon of cybercrime is growing and becoming increasingly complex, **there is no adequate capacity at EU level to tackle it**. Two main factors may be identified as contributing to the problem.

2.1 Cybercrime is extremely complex, evolves very rapidly and requires high-level technical expertise to understand its characteristics and modus operandi

Cybercrime is a term that is used to refer to a broad range of different activities relating to the misuse of data, computer and information systems, and cyberspace for economic, personal or psychological gain. Policy-makers at the EU and at national levels, academics and law enforcement practitioners have put forward different definitions and systems classifying cybercrime. The following activities are commonly understood to be types of cybercrime:

- Hacking / Intrusion
- Distributed Denial of Service
- Attacks against critical infrastructures
- Botnets

- Malware and spam
- Scams and online frauds
- Phishing
- Identity theft and identity fraud
- Advance-fee fraud conducted Attacks (DDoS) over the Internet
- Online harassment
- Production, distribution and downloading of child abuse material
- Virtual cybercrimes

While some forms of cybercrime present totally new scenarios in view of the context in which they are committed, other forms have parallels in traditional forms of crime, but may include additional complexities due to their digital dimension.

Overall, the phenomenon of cybercrime defies simplistic understanding, evolves rapidly in line with ways in which society uses cyberspace and requires technical knowledge to understand it. The mapping of long-term trends and patterns is therefore complex.

The technical sophistication required to tackle cybercrime comprehensively means that traditional ways of investigating this kind of crime are inadequate. Law enforcement services need to undergo a high level of IT training to understand the intricacies of the technology involved and keep up with its rapid changes, the new landscape of digital forensics and the fast-changing modus operandi of cybercriminals. Unless they do so, the EU's capacity to tackle cybercrime adequately will continue to lag behind and the gap could grow even wider than it is at present. Fast-changing technology has to be matched with fast-changing technological tools that can be deployed in the fight against cybercrime, with personnel capable of adapting and building on previous knowledge and expertise.

2.2 Insufficient flow of information

Highly-skilled expertise gained at national and EU level needs to be exchanged among all Member States so that the EU can improve its response to cybercrime, a phenomenon which is inherently of a cross-border nature and therefore requires cooperation. However, information does not flow efficiently enough at present. Various factors may account for this.

The first is of a cultural/sociological nature and manifests itself at both national and EU level (ie in relation to Europol). Member States have not been forthcoming in sharing cybercrime information with Europol, though there are signs that this is slowly changing. Reticence to use Europol as a focal point for information exchange is probably due to factors such as a policing culture that is cautious about sharing information, has low awareness and lacks knowledge.

Lack of precision in the legal provisions and organisational factors can also explain the lack of use of Europol channels for exchanging information. Europol National Units are organised differently within different Member States' law enforcement landscapes, and this has an impact on each Member State's performance and effectiveness. This problem is not exclusive to the area of cybercrime and tends to arise in most areas in which Europol is active. The

perverse effect is that the less information Member States share, the less relevant data Europol has within its databases that could be useful to Member States' own investigations if it were shared.

The second reason hampering the flow of information is of a more structural nature. Until recently, most Member States did not have structural links with the private sector for the purposes of fighting cybercrime. This meant that few cybercrime incidents reports reached the national law enforcement agencies. This made the gathering of digital forensic evidence problematic. Since the private sector owns and runs most of the internet structures in the digital landscape where cybercrime takes place, it would be more effective to depend less on sporadic cooperation and more on solid structural collaboration. National/Governmental Computer Emergency Response Teams (often known as CERTs) have started to fill this gap and already provide an important interface between public authorities and private stakeholders at national level. However, this is not sufficient, as public-private partnerships should extend over a wide range of issues and not be restricted solely to emergency response situations.

A third factor is partly structural (for instance, inadequate channels in place for individuals to file reports), partly cultural (lack of awareness regarding sanctions against new forms of crime) or from incentives not to report (for instance, the scale of the loss suffered in relation to the complexity of informing the authorities, or an organisation's legitimate fear that its reputation might be tarnished or its actions be put under the scrutiny of the data protection agencies who might investigate them for not securing clients' data adequately).

The same problems are reflected at EU level. The current legal framework governing Europol does not allow it to share information directly with the private sector. A business has to go via a Member State LEA, which may report to the Europol National Unit set up in that Member State, that in turn reports to Europol. This clearly imposes unnecessary burdens on multi-national companies that have to inform various LEAs, with Europol depending on each of the intermediaries at Member State level for information. This structure is often a reason for substantial delays, or even loss of information, for all types of crime.

Having an efficient information-sharing system is even more critical in the area of cybercrime, where an immediate response e.g. to a cyber-attack or an exchange of information is vital. The two main factors that contribute to the problem defined earlier have a common end-result which is: less cybercrime resolved, resulting in more EU citizens becoming victims, and more losses to the economy. Eventually, this erodes public trust in the internet-mediated economy, damaging the EU's growth in an economic sector where it is considered a leader.

If no action is taken, the consequences could be rather serious. It can be assumed that cybercrime would continue to increase, both in terms of volume of malicious activity and in complexity. With the current lack of adequate capacity to fight cybercrime, it would continue delivering significant blows to the EU's economy and seriously prejudice the well-being of EU citizens, as more persons and businesses become victims or targets of cybercrime.

The Commission's Feasibility Study revealed a general growing trend in cybercrime, based on data collected from specialised cyber units within the law enforcement agencies of a number of Member States. Failure to contain the threat that cybercrime poses to the EU's internet-mediated economy in the current challenging economic situation could hamper the EU's efforts to emerge from the crisis.

2.3 Added Value of EU involvement

The European Cybercrime Centre is being established to overcome the many obstacles to the effective investigation of cybercrime and prosecution of offenders at European level. It is a key step in the EU's overall strategy to improve cyber-security and to render cyberspace an area of justice where human rights and fundamental freedoms are guaranteed through the cooperative efforts of all stakeholders.

Because of the transnational nature of cybercrime, facilitated by the inherent borderless nature of the internet, the EU's role in coordinating efforts, extracting best practices, pooling expertise, tapping synergies and avoiding duplication is indispensable.

The EC3 will significantly bolster the EU's capacity to confront the growing, complex threat posed by cybercrime, with a view to supporting and complementing Member States' efforts far better than current capability. It will provide better operational support capacity at EU level for cross-border cybercrime trend forecasts, threat assessments, as well as providing training and capacity building for staff to tackle complex cybercrime cases.

Member States will benefit significantly from having a focal point equipped with state-of-the-art technology and a highly-qualified, specialised workforce offering a wide spectrum of services and products to complement Member States' own efforts in fighting technologically-complex transnational crime.

The centre will thus have an important coordinating role in terms of operational support, and will act as a hub within which information on cybercrime from numerous sources is processed 24/7. It will also be forward-thinking, anticipating trends, analysing threats and providing forensic support, training, and strategic guidance towards tackling cybercrime that will be of enormous value to Member States.

EU agencies will see their capacity to address the challenges raised by cybercrime significantly bolstered.

Europol, as the pre-eminent organisation charged with addressing serious crime and terrorism at European level, will have a stronger mandate to conduct intelligence-gathering and analysis to support law enforcement personnel in the Member States.

Eurojust will benefit from the EC3, fostering inter-disciplinary expertise on cybercrime, better awareness and knowledge of investigative tools, as well as procedures and digital forensics for evidence purposes. Improving contacts between Europol and Eurojust should lead to aligning criminal investigation considerations with judicial/prosecutorial needs in an area that is new and technologically complex for practitioners.

There is scope for many synergies between the converging interests of cybersecurity and fighting cybercrime. The creation of the EC3 therefore benefits ENISA and the EUCTF in terms of identifying strategic priorities.

Finally, the EC3 will enable European cybercrime investigators on the international scene to have a collective voice, for instance, in discussions with the ICT industry (which is global in nature), Interpol's cybercrime activities (a Digital Crime Centre in Singapore is planned for

2014), other international police cybercrime units and UN or other international organisations.

3. Objectives

General Objective: To strengthen the EU's capacity to tackle the complex and constantly-evolving nature of cybercrime with a view to avoiding significant harm to individuals and businesses which can result in major losses to the economy and erosion of EU citizens' confidence in the internet.

Specific Objectives:

- To enable more extensive, faster information exchange among all stakeholders (Member States, third countries, LEAs, industry etc.) and more effective management of information flows (i.e data fusion, helpdesk and reporting mechanisms)

- To assist Member States' investigations through more substantive operational support for trans-national organised cybercrime

- To provide extensive, specialised, tailored training to all stakeholders, particularly the law enforcement community within the EU and beyond, in cooperation with CEPOL, where appropriate; to collect, collate and disseminate best practices among stakeholders; stimulate R&D in the area that can translate into practical tools for fighting cybercrime

- To establish a collective voice for the cybercrime investigator community, internally within the EU and on the international scene, through outreach, policy support/strategic direction and regular cybercrime-related threat assessments and trend forecasts/analysis.

Operational Objectives:

Ensure that the EU has the necessary infrastructure to deliver its activities effectively with minimum costs for the EU budget. Such an infrastructure implies:

- sufficient human resources

- sustainable funding, particularly in view of the Multi-Annual Financial Framework discussions for the period 2014-2020

- necessary IT infrastructure and capacity and accompanying highly-skilled expertise required to carry out the tasks

- inclusive governance structure in relation to the EC3's Programme Board, responsible to advise EC3 management (which ultimately answers to Europol's Management Board).

4. Policy options and Risk Assessment

Five different options (including the status quo) were assessed in the light of the objectives identified and against the criteria of effectiveness, efficiency and coherence.

- **Option 0: Maintaining the status quo**

- **Option 1A: The EC3 is set up within one of the existing EU agencies, ie:**
  - **(a) Europol**
    - **i. owned by Europol**
    - **ii. hosted but not owned by Europol**
  - **(b) Eurojust**
  - **(c) ENISA**
- **Option 1B: The EC3 is set up through the creation of a new agency specifically for this purpose**
- **Option 2: EC3 is set up as virtual centre**
- **Option 3: One Member State runs the EC3 on behalf of the EU**
- **Option 4: EC3 is set up as a public-private partnership (PPP)**

Option 0: Maintaining the status quo

No EC3 would be established and activities would continue as now, with various EU institutions currently addressing cybercrime. It is expected that efforts would continue towards integrating the High-Tech Crime Centre (HTCC) in Europol within its Operations Directorate, subject to the next administrative re-organisation associated with the new AWF structure and the upcoming new Europol Regulation. Eurojust would also continue to support the judiciary and public prosecutors and work with Europol on joint investigation teams (JITs). Furthermore, training efforts would continue as now, with CEPOL and ECTEG both delivering different types of training aimed at different customers. Finally, ENISA's CERT coordination program would develop and refine its interpretation of how to establish cooperation with the CERT community, building on the first CERT–LEA workshop, held in October 2011.

Analysis

Under the status quo, the lack of adequate capacity to tackle the growing, complex problem of cybercrime would remain the same. Europol would continue registering sporadic successes, but the strain on its resources as Member States request more operational support would result in more rejections on Europol's part, denting trust in Europol's capacity to respond to transnational cybercrime and a general failure to respond to the cybercrime threat within the EU.

Option 1A: The EC3 is set up within one of the existing EU agencies, ie:

(a) (i) owned and run by Europol

In this option, the EC3 would be anchored within Europol's legal framework and would be ultimately responsible to the Europol Management Board. Structurally, it would be identical to any specialised unit within Europol, such as the HTCC, but EC3 would have a Programme Board made up of a number of identified stakeholders to fulfil the comprehensive approach

envisaged by EU institutions. The Board would be in charge of its general steer and strategic direction.

Given Europol's current mobile forensic capabilities, network and links to Eurojust, Europol could provide operational investigative support apart from general collaborative support on cybercrime issues that Member States might require in their general work. Achieving the objective of intelligence-sharing would also be of an operational nature, since Europol already has a well-established intelligence apparatus in the form of the AWFs.

With regard to outreach, this would be envisaged as collaborative rather than operational in nature, given the current legal framework as to what can and cannot be shared with the private sector.

The role of Europol in being a point of strategic advice would necessarily be advisory in nature (as this would involve collecting and collating the views of different Heads of HTCUs across Europe). Similarly, contact development would be achieved in a collaborative way at Europol, via sharing information and working alongside national HTCUs and other partners (e.g. private sector). Running an internal 'one-stop shop' hotline could be an operational activity (in the same way as the current intelligence databases). Finally, to achieve the objective of training, it would work with other training partners (such as CEPOL, ECTEG, academia and industry), noting that Europol also provides some specific, targeted training of its own (e.g. in investigative techniques). Europol has also signed different types of cooperation agreements with third countries (permitting the exchange of personal data) and institutions (e.g. Interpol).

Analysis

As the EU's only criminal intelligence agency, Europol has a clear mandate in this domain and is a well recognised 'brand' among Member States and other stakeholders (e.g. Interpol, non-EU countries and the private sector). In addition, Europol has for some time had a strategic intelligence and analytical capability in the domain of cybercrime, via its HTCC. This has taken some time to develop since 2009. This internal 'centre of gravity' is also bolstered by the skills, knowledge and capability of intelligence analysts from the Operations Directorate who work on the cybercrime-associated AWFs Cyborg, Twins and Terminal. The legal basis of the agency is tailored to its operational support role — it has an extensive and very robust data-protection regime and a complex set of rules governing participation in the AWFs.

This legal basis is currently under revision and might in future offer further flexibility on exchanges of data with external partners, including the private sector. From the perspective of infrastructure, Europol has a brand-new purpose-built physical headquarters and an extensive ICT establishment including a data centre, secured network and forensic facilities. Under this option, Europol needs to receive additional resources to set up and run the EC3 in addition to its existing appropriation. These resources would concern mainly staffing, since extensive physical and ICT infrastructure (as described above) is already in existence, making this option highly cost-effective.

Under the current legal framework, private sector actors can transmit to Europol data regarding technical information on crimes actually suffered or anticipated. This data, in turn, can enable Europol to identify crime patterns or 'modi operandi' of criminals or new trends. As regards personal data, Europol can receive this from the private sector only indirectly, i.e. if

transmitted by the competent Europol National Unit (ENU) or, if the private party is based in a third country with which Europol cooperates, via the designated contact point in that third country. Experience shows that this rule often causes delays in Europol receiving data, or even has a deterrent effect.

Risks

The fact that the current legal regime prevents direct cooperation between Europol and the private sector would be a potential stumbling block.

The proposed revision would allow Europol to share its strategic and technical data with private parties, including data from confidential sources. Such sources often attribute their low level of cooperation with LEAs to the one-way flow of information (from private parties to LEAs) and cite the lack of feedback from LEAs on interesting findings or assessments that would enable private parties to be more effective in preventing and handling cybercrime. This amendment would improve the effectiveness of the EC3 and improve the flow of information.

Focus on the intelligence and investigative organisational character of Europol could create barriers to the deeper cooperation with other stakeholders needed to achieve the broader strategic goal of building up a bigger picture of the extent of cybercrime. This risk could be neutralised through having a Programme Board with a broad membership that reflects the full spectrum of relevant stakeholders and through a management that takes into account the interests of all members and prioritises the cooperative approach.

(a) (ii) The EC3 hosted but not owned by Europol

Analysis

Under this option, the EC3 would have its own mandate, though limited by Europol's mandate on whose supporting infrastructure it would rely. The existing facilities, infrastructure and 'brand name' of Europol would be leveraged by the EC3. However, the EC3 would have a separate legal personality, budget and an explicit mandate to cover specific types of cybercrime, which may be different to that currently defined in Europol's governing legal instrument. To a large extent, it would be able to conduct the same sort of activities as an EC3 owned by Europol. Additional oversight would be necessary, bringing in perspectives from other organisations (e.g. Eurojust, ENISA, CEPOL). This oversight might be a necessity if the EC3 were to process sensitive personal data (also known as nominal data) in the criminal intelligence aspect of activities supporting Member State level investigations. Such oversight would also need to extend to governance of the EC3 to act as a natural counterbalance to any possible institutional inertia and to help ensure that the EC3 delivers according to its mandate.

In terms of resources, an EC3 hosted by but not owned by Europol would not require investment in significant capital-intensive items such as a data centre, secured network, information system or extended computer forensic network. These could be 'hired' by agreeing internal Service Level Agreements (SLAs) between the EC3 and Europol. The EC3 might pay a sum each year (a percentage of the capital investment in these infrastructures) in return for which it would be allowed to use the resources.

Risks

Such an option would entail the risk of developing an 'agency within an agency' and might have the perverse effect of the EC3 being seen as a law enforcement competitor to Europol. Separate operational agreements would have to be established — such as those Europol now has with other organisations, e.g. Interpol — to allow personal data to flow between the AWF infrastructure and the strategic intelligence activities of the EC3. Risks would include those of visibility and the perception of the EC3's role within the broader criminal justice and private sector communities. This is particularly important in an area such as cybercrime, where the engagement of the private sector is highly important. The end result might be sub-optimal for both Europol and the EC3, since it would take time for the EC3 to establish its credibility, while Europol's might be undermined.

The bureaucratic complexity required to separate Europol (with a possible future mandate to address many different types of serious and organised crime, except cybercrime) from the EC3 (focused solely on cybercrime) would undoubtedly be complex and would require further interaction through other governance mechanisms. The future Europol legal instrument would need to have cybercrime deleted as a type of serious crime. A legal instrument for an EC3 would thus need to define the types of cybercrime that would be within its competency.

(b) The EC3 hosted by Eurojust

Analysis

Many aspects analysed with respect to Europol are also relevant to Eurojust, which already operates Mutual Legal Assistance Treaties (MLAT) support functions and joint investigation teams so achieving this objective would have an operational nature. This option could present similar advantages to the 'Europol as a host' option, namely known brand-name, long-established agency with operational functions.

However, providing criminal intelligence functions would have to be collaborative, since Eurojust would need to rely either on the intelligence capabilities of Member States or of others such as Europol. Outreach would have to be collaborative in nature, leveraging the capabilities of stakeholders who have more public presence in the domain. The provision of strategic advice would need to be advisory, as above, as it would require the collation of views from Member States. Concerning the development of contact points, Eurojust would be able to achieve this in a collaborative or operational approach — either by building on its own network, or via linking to others (for example, the G8 24/7 network or the EU Working Group on High-Tech Crime at Interpol). An internal support hotline or one-stop shop could run through operational means, as is done now. Finally, as regards training, this would be necessarily of a collaborative or advisory nature (e.g. working alongside training providers or pointing Member States in the direction of other stakeholders who offer training) since Eurojust does not currently carry out any training activities.

Risks

As an agency with a judicial remit, Eurojust would be legally unable to represent the views of an operational police community, which would be a serious risk. Furthermore, Eurojust would have to rely heavily on MS and Europol to provide any intelligence functions.

(c) The EC3 hosted by ENISA

Analysis

As ENISA is the only 'core' EU-level stakeholder with a non-operational function, achieving many of the objectives identified from the empirical evidence base would take the form of collaborative or advisory activity rather than direct operational intervention. The one area in which ENISA could take an operational role is in delivering training (since the Agency has already delivered exercises and also delivers training for LEAs and CERTs). Outreach could be performed more collaboratively, since ENISA already has better links with many of the non-law enforcement stakeholders (especially private industry) than the other current EU-level stakeholders.

Risks

It would be highly unfeasible for ENISA to undertake direct investigative support or intelligence sharing, since these are tasks for which the agency has no competence and no mandate.

Option 1B: The EC3 is set up within a newly-created agency specifically for such purpose

Analysis

Under this option, a new structure, possibly with its own premises, staffing, budget, legal basis and infrastructure would need to be established.

Given this relative freedom, such an agency might be expected to 1) create or 2) lift out and assume the operational implementation of different measures regarded as being of importance. For example, addressing the objective of supporting Member State investigations into cybercrime would be done in a collaborative or advisory way, offering resources (e.g. mobile forensic labs) to Member States. Similarly, achieving the required intelligence capability would be best served in an operational or collaborative fashion, either running an intelligence database (as under the Europol model) or leveraging the intelligence capabilities of Member States. The remainder of the tasks could be undertaken on an operational basis since the mandate of a unit could be designed specifically around implementing measures to address these objectives. For example, the 'on call' facility of Eurojust could be housed within a new EU agency (which would require Eurojust surrendering the resources required to implement this). Similarly, a new EU agency could easily assume the functions of training as provided by CEPOL and ECTEG (and even implement measures to obtain certification from an independent academic institution).

Risks

The risks of this option are mainly financial (major costs of setting up a new agency), the length of time it would take for a legal instrument establishing a new agency to be adopted under EU decision-making rules, as well as the added hurdle a new agency would face in establishing itself within an already rather crowded landscape in the area of criminal justice and ICT-related matters.

Option 2: The EC3 is set up as virtual centre

Analysis

Given the differing competencies, perspectives and legal bases of each relevant organisation, a virtual EC3 would aim to link up the organisations to deliver an overall capability, without seeking to create a wholly new organisation. It would nonetheless require some modification to existing structures and might have additional administrative and bureaucratic implications (in establishing frameworks for interoperability between the existing stakeholders).

Such a virtual centre would leverage existing capabilities in each relevant stakeholder (for example, Europol's intelligence capabilities, provision of investigative support, etc.) in an advisory capacity (e.g. directing queries to other, better-placed stakeholders).

This would be immediately practicable since it would require fewer legal amendments. It might also secure political acceptability, as it would not require setting up new structures or a new agency. A virtual ECC would also be much less resource-intensive to establish compared to the high set-up costs of a new data centre, intelligence machinery and forensic suite. This option goes slightly further than the option of maintaining the status quo.

Links and relationships with other stakeholders would need to be modified, for example by drawing up operational cooperation agreements between ENISA and Europol — which might require amendments to ENISA's governing regulation, allowing it to process personal data. This would entail less work than creating the legal basis for an entirely new organisation.

Given the broad nature of the activities envisaged for an EC3 (as discussed above), a virtual EC3 is attractive because it leverages the expertise and competency of each organisation without requiring additional capacity or capability.

Risks

There are some significant operational drawbacks to setting up a virtual centre. In general terms, if the EC3 does not have a centre of gravity by virtue of being hosted within a specific organisation, many stakeholders may view it as similar to the 'status quo' option. This would not necessarily be the case, as despite being a virtual EC3, it would need a small governance team that would have to be located somewhere, with possible resource implications. A virtual centre would therefore still incur some costs and might also be expected to sign SLAs for use of certain capital-intensive resources owned by Europol (subject to specific rules governing sensitivity and security, for example). Furthermore, the lack of a single institution or organisational host would mean that the positions or perspectives of each stakeholder would not be challenged and existing institutional inertia may conflict with any attempt to work collectively for a common goal.

The main difficulty with this option would lie in the overall guidance needed, which would imply some form of collective board or decision-making authority to ensure that each stakeholder is incited to accept responsibilities, contributes fairly and works collectively and collaboratively, drawing on capabilities within their respective organisations to address problems jointly. This would also suggest that an independent non-partisan and expert chair would be required to marshal the efforts of these organisations.

The mandate of a virtual ECC would be similarly complex and broad. Unlike a mandate for an EC3 hosted by Europol, for a virtual ECC, this would require negotiation between the four main stakeholders to establish where there was enough overlap and consistency between the governing rules of each, to draw up a new mandate that would be compatible and enable

each relevant organisation to play its part. ENISA has been focusing on best practice concerning Critical Information Infrastructure Protection (CIIP) through its role in the EP3R (European Public Private Partnership for Resilience) and its CERT cooperation team helps to facilitate best practice across all types of CERT.

Option 3: One Member State running the EC3 on behalf of the EU

Analysis

Under this option, a single Member State would be responsible for the operational running of a new agency, on behalf of the Union. In view of the specific legal, contextual and administrative structures that would be required, the only pragmatic solution would be that to achieve certain objectives. A collaborative or advisory approach might need to be taken — for example, running an intelligence database or providing investigative support. However, in other less controversial domains (for example, outreach to different stakeholders — members of the public, industry, etc.) a Member State could take a much more operational role on behalf of others.

Risks

The precedent for this option is the management agency for the second generation Schengen Information System (SIS), run by the French government (and staffed by French law enforcement officials) on behalf of the rest of the Union. This option would be suited to an EC3 with a clearly defined technical role — for example, specifically for the running of an online reporting platform, rather than the type of EC3 set-up that has been discussed in detail above.

Option 4: The EC3 set up as a public-private partnership (PPP)

Analysis

In this option, a PPP would be set up which would potentially require the establishment of a new administrative structure.

A PPP would include measures already undertaken to achieve objectives as described earlier (such as intelligence provision, investigative support and coordination) which could be either undertaken in-house or via leveraging existing strong capabilities. A PPP would also (by its nature) be able to engage more closely with non-law enforcement players (such as the private sector, academic training partners) to meet some of the requirements identified from fieldwork.

Risks

Although surmounting the incentive structures to obtain engagement from the private sector (particularly with respect to intelligence exchange) is clearly not a trivial task, the ‘clean sheet’ approach of a PPP could support such interaction.

It is notoriously difficult to establish public-private partnerships due to the diverging interests of private authorities and public authorities, and they are heavily dependent on the willingness of the private sector collaborating effectively.

5. Comparative analysis of the Options

The detailed analysis above has shown that some of the proposed options would fail the effectiveness test in terms of meeting the key objectives of setting up the EC3.

Options 1A (b) and **1A (c)** (the EC3 hosted and/or run by Eurojust or ENISA) are not likely to be feasible in view of the existing mandate of these two agencies. Eurojust's strict judicial remit would mean a big hurdle to overcome to enable criminal intelligence gathering, while ENISA lacks any operational responsibilities and does not possess a mandate in the field of cybercrime**.**

Option 1B, (setting up a new agency) has many drawbacks, such as the length of time it would take to set up, the crowded landscape of agencies in the criminal justice area at EU level and the very high cost involved in setting up a new EU agency.

Option 3 (one Member State running the EC3 on behalf of the EU) has in the past only worked in the case of a limited technical role and is not suitable for the EC3 set-up envisaged.

As regards **Option 4** (setting up a public private partnership), while PPP is a laudable goal to pursue in terms of general policy, the possibility is also discarded in view of its high risk of failure.

We are thus left with the following three options to compare with the baseline scenario, options 1A (a) (i), 1A (a) (ii) and 2.

These shortlisted options have been assessed against the following six criteria (more details on the comparison are provided in Annex 1):

- ✓ Mandate
- ✓ Resources
- ✓ Activities
- ✓ Risks
- ✓ Cooperation
- ✓ Impact

Assessment / Options	Effectiveness				Efficiency		Risks	
	Human Resources	Sustainable funding	IT Capacity	Governance	Time Needed	Costs of setting up the Centre	Mitigation of exposure to data protection infringements	
Option 0	0	0	0	0	0	0	0	0
Option 1A(a)(i)	+	-	++	+	++	3.5 million eur	++	++
Option 1A(a)(ii)	-	-	- -	+	-	10 million eur	+	-

Option 2	+	-	0	-	+	1.5 million eur	-	-

Magnitude of effectiveness and efficiency: ++ strongly positive; + positive; 0 neutral; — negative; — — strongly negative

N/A not applicable

Figures included in the column on costs cover one-off expenditure and not the running costs of the Centre.

The table shows that **Option 1A(a) (i)** (EC3 hosted and owned by Europol) is the strongest option, particularly due to readily available human resources, physical and IT infrastructure and a very robust data protection system already built-in, absolutely crucial to achieving the objective of a more efficient information flow.

Option 2, which appears as equally strong in terms of available human resources and the time needed to set up the EC3, would imply setting up a new data protection system, with all the difficulties and risks attached to that in terms of ensuring sources of data have confidence in the system, and, subsequently, its effectiveness in terms of data sharing. This is a serious flaw in the effectiveness of this option.

An EC3 owned and run by Europol is therefore the most effective and feasible option. Nevertheless, a more detailed cost evaluation is necessary, considering that the level of resources dedicated to the EC3 will strongly influence its capacity to deliver and match the objectives set out in the Commission's Communication.

6. Evaluation of the costs implied by the chosen option

The following table categorises and lists the type of resources to be considered:

Item	Description
Labour	Costs to employ personnel for one year, including salary, pension, social security contributions etc.[5]
Non-Labour	ICT desktop equipment Training Travel and expenses Co-funding Services

[5] It should be noted that staff occupying restricted posts in Europol are only allowed to serve a maximum of 9 years without possibility of extension. This limitation is due to Europol's specific legal framework and is unique when compared to other EU agencies. Thus, future liability in relation to indefinite contracts and subsequent pensions does not arise. .

	Software development Software maintenance Studies and research Translation Research & Design and communication

Since Europol has its own physical structure and an existing ICT infrastructure, there are no costs arising from rental facilities or capital-intensive investment on ICT infrastructure. These are in fact huge savings that were considered when comparing the options available.

Allocation of costs

Against the types of activities that are envisaged for the EC3, costs can be allocated as follows:

Activity	Labour	Non-Labour
Governance — general management of the EC3, liaising with Programme Board members, identifying and setting priorities, relations with Europol's Management Board	Cost of staff to fulfill the governance function of running the EC3, the EC3 Programme Board, liaising with members of the Programme Board and providing general administrative support	ICT desktop equipment, travel and expenses; services; studies and research; design and communications
Data Fusion– synthesise public and private information flows, respond to incoming requests and to coordinate action by the relevant team(s)	Costs of staff to handle vast flows of information from a variety of sources; Costs of staff to develop and manage a cybercrime reporting software application	ICT desktop equipment; research and design; IP software rights
Operational support for investigations — operational analysis and coordination, cyber-attack response, intelligence development, financial investigation and forensic	Costs for trained analysts to analyse criminal intelligence data and provide ongoing operational and forensic support to MS LEAs	ICT desktop equipment; services

support		
Training — including identification, together with CEPOL of gaps in knowledge and needs assessment, developing (in cooperation with CEPOL and ECTEG where appropriate) specialised and tailored training programs and tools, collecting and disseminating best practice	Costs of staff to identify training needs, develop training programs and tools, identify best practice, collate and disseminate it	Training, travel and subsistence; studies and research; translation
Outreach and policy support Public Private Partnerships, outreach towards the research community, centres of excellence, CERTs, crime prevention, policy work and strategic planning, trend analysis, early warning and horizon scanning, trend forecasts	Costs of staff for conducting general outreach, strategic and policy work	Travel expenses; cost of necessary ad hoc infrastructure/platform within which cooperation can take place

6.1 Human resources

The Commission's Communication on the Establishment of a European Cybercrime Centre (28 March 2012) noted that when assessing estimated resource needs, the Commission would be guided by the following three considerations:

1. ***the increase in the total cybercrime caseload*** *would be moderate*
2. ***Member States would enhance their own capability*** *to fight cybercrime*
3. The EC3 would only deal with a ***certain set of cybercrimes***

The above assumptions imply that some form of prioritisation will always have to take place. At present, Europol responds to almost 10 000 requests for operational assistance on cybercrime a year. Such assistance may vary from a mere request to cross-check information with investigations in other MS, to requests for information pertaining to joint investigations, to requests for specialist technical and forensic support. This significant range has an important impact on the resources required. A distinction is thus drawn between:

- **High profile operations**: Operational work providing substantial support to at least two Member States but often involving several Member States and/or third countries (sometimes more than 20), with a continuous exchange of information for a prolonged period

through the delivery of at least one of Europol's products and services, but often involving a range of services such as exchange of operational data, analysis and technical support, operational meetings and the exchange of many SIENA messages. Such complex cases involve the work of at least one Europol officer for 6 months/1 year and sometimes even 1.5/2 years.

- **Standard operations/cases**: Operational work providing support to MS through the delivery of at least one of Europol's products or services. A standard operation may comprise one SIENA message involving only a cross-match report.

It is useful to bear this distinction in mind when considering 'cybercrime case handled'. While the importance of standard operations is not to be underestimated, it is clear that the EC3's success will be measured to a far greater extent by the number of high-profile operations involving transnational organised cybercrime groups operating within and beyond the EU, similar to Europol's crucial operational support in *Operation Icarus* in which 273 child sexual abuse suspects were identified and 113 of those suspects spread across 23 countries were arrested.

The analysis below is based on work done by the Commission that draws on the Feasibility Study, as well as on Europol's needs assessment. The calculation is meant to meet the objectives set out in the Commission's Communication. An analysis of the tasks of each of the EC3's five sub-units should help to explain the rationale behind resources needed.

Operations: Operations performs the coordination of large cybercrime operations (or investigations), operational analysis and support, technical and digital forensic examinations (including on-the-spot). It specifically coordinates complex transnational cases to avoid the overlapping and duplication of efforts among cybercrime units in Member States and partner countries.

Personnel working on each of the three former Analytical Working Files[6] (now called 'focal points') are currently distributed evenly, with staff working on each. Europol presented statistics to the Commission that show the low ratio of personnel per high-profile operation. These explain the current limited delivery in operational support (including having to reject or delay support to online child sexual abuse cases). The Commission thus agrees that boosting the capacity of operational support is fundamental to enable Europol to handle more high-profile operations.

Data Fusion: This refers to collecting and synthesising information from various sources to provide a comprehensive cybercrime picture to all other teams in accordance with the relevance of that information to their work. Apart from a fully-fledged one-stop-shop for processing of all cybercrime-related information coming through, the data fusion function

[6] Analysis Work Files are intelligence databases that Member States can submit information to, and request information from. The objective of these databases is to support on-going investigations or initiate new cross-border cases. This is accomplished via building a cross-border picture on active groups including information on their modus operandi, routes for money and sequence of events. In the field of cybercrime 3 AWFs are of relevance: TWINS (child sexual abuse online), TERMINAL (credit card fraud), CYBORG (intrusion). The AWF structure will disappear in view of the creation of a single database on organised crime, but the EC3 will maintain these 3 work-streams, to be re-labelled Focal Points..

could also involve a 24/7 support function, malware analysis, attack monitoring, alert, internal security monitoring, helpdesk, operational coordination, etc.

The data fusion function is also fundamental to the success of the EC3. In terms of data handling, pro-active scanning of the cyber environment and logistical support to all other teams, this will mark a relevant change from the way Europol has been tackling cybercrime thus far. The 24/7 support function which Europol proposed to roll-out in 2013 (and which would require 7-8 personnel to manage) can be delayed until the EC3 achieves cruising speed.

Outreach: The Outreach and Communication teams manage relationships with stakeholders in the Private Sector, Academia and Third Parties. This activity will be vital to create sustainable public-private partnerships and dialogue and is crucial to the concept of the EC3 bringing various communities (law enforcement, computer emergency response teams, industry etc.) together.

The first priority is to ensure the EC3 virtual platform SPACE (Shared Platform for Accredited Cyber Experts) functions efficiently and that any exchange or personal data is framed by sound data protection safeguards. This enables easier exchange and sharing of strategic and technical knowledge and expertise among all interested stakeholders. With time, the EC3 will increasingly become the collective voice of cybercrime investigators in the EU. It will communicate EU views, positions and results in the area of cybercrime; become the EU Central Office for Cybercrime; coordinate EU Member States and EU agencies' inputs to internet governance and promote standardisation of approaches and adoption of good practice in the field of cybercrime. The EC3 will also deliver tailored newsfeeds on emerging criminal trends, technological developments and other relevant information as it develops. These will be informed by active partnership with research institutes, academia and industry partners.

R&D and Training: This team is devoted to research on technical threat analysis and vulnerability scanning, static forensics, best practice and training and the development of tools, including tools for digital forensics. In cooperation with CEPOL and ECTEG (European Cybercrime Training and Education Group) as well as with Eurojust, private companies and research bodies it will contribute to the design and delivery of cyber-related training.

A cost-effective approach must take advantage of synergies with other players such as the EU's Joint Research Centre (JRC), CEPOL and ECTEG (for training). The EC3's primary role is to streamline training, provide valuable input and align it with its strategic products. An important leap from the current status quo is offering key services in cyber forensics. Most Member States view the EC3 as a crucial point of reference on digital forensics, since only a few large ones have developed any capacity in the field. Digital forensic evidence is essential for the successful prosecution of cybercrime cases, so activities to enhance this capacity to support Member States require more resources.

Strategy and Prevention: The Strategy team conducts trend analysis, early warning and horizon scanning, crime prevention, policy work and strategic planning. The analytical level of this unit aims to help partners and stakeholders improve their understanding of cybercriminal activity and methods, and to anticipate developments.

Delivery of strategic products to enhance the knowledge-base on cybercrime within the EU criminal justice landscape is a very important function. Additional personnel should contribute to providing a forward-thinking Centre that forecasts trends and assesses threats so as to improve the EU's overall capacity to prevent and respond to cybercrime and feed into the Commission's policy-making. Through its outreach work towards civil society, preventive work can be achieved through, for instance, awareness-raising campaigns. The Commission can also play an important role in this and supplement such work through its funding programmes and by ensuring proper alignment with the work of the EC3.

In calculating the needs for human resources, the underlying rationale is that a significant surge is needed in the first years, until the EC3 achieves cruising speed in 2015. After 2015, provided there are no major and unforeseen changes in the nature of cybercrime, the increase in personnel could level off. Below is a detailed table of anticipated human resources needs between 2014-2020:

Table: Commission projections for the number of human resources required each year for each of the EC3 teams until 2019:

	Strategy and prevention	**Outreach and communication**	**R&D and training**	**Operations**	**Data fusion**	**Management**	**TOTAL**
2012	4	2	1	22	1	1	31
2013	4	3[7]	4	26	3	4	44
2014	5	5	8	33	4	6	61
2015	6	6	10	43	11	6	82
2016	7	6	11	45	11	6	86
2017	7	7	11	48	11	6	90
2018	7	7	12	51	11	6	94
2019	7	7	13	53	12	6	98

The need for more non-human resources

Although Europol's physical infrastructure is sufficiently equipped for the EC3 to start operating immediately, certain costs that are specific to creating it will still be incurred and need to be factored into the cost-calculation assessment. For this purpose, a difference is drawn between administrative expenditure and operational costs. The former relates to building-related costs, facility and IT equipment, while the latter refers to the day-to-day

[7] EC3 may get an extra SNE but this is not ascertained yet. It is provisionally calculated however. .

running costs for missions, meetings, consultancy, training, software upgrades and IT maintenance.

The table in Annex 2 shows the financial resources needed for the EC3 between 2014 and 2019.

It is important to note that this calculation has been made using the simplified method proposed by DG BUDG — average costs of an official = 127.000/year. Furthermore, the assumption is that staff will be recruited in July each year.

It must further be noted that for the purposes of this calculation, the **current 31 staff** working on cybercrime within Europol **and the extra 12 positions** (5 posts + 7 new vacancies) that Europol will reallocate during the course of 2013 are already covered by the current Europol budget. In other words, the salaries of the 43 personnel (existing 31 + reallocated 12) expected to work within EC3 in 2013 **are not factored** into the calculation. However, all additional staff from 2014 onwards are factored in.

7. Planning future monitoring and evaluation

Indicators

Below is a table that establishes a format for assessing the success or otherwise of a European Cybercrime Centre:

Field of Intervention	Output Indicators	Result Indicators	Outcome / Impact Indicators
OPERATIONS **Identification / disruption / dismantling of cybercrime networks and cybercrimals**	**No. of operations supported (distinguishing between high-profile and standard operations)** **No. Joint Investigations Teams (JITs)supported by EC3**	**No. of suspects identified, arrested, prosecuted in MS in cybercrime / no. of victims identified** **No. of cases handled by JITs**	**EC3 impact on disrupting cybercrime networks and helping MS arrest cybercriminals / MS satisfaction rate of EC3 operational support**
Information Sharing	**No. of contributions received (from MS, third parties academia, CERT, private sector)** **Volume of data received** **No. of helpdesk requests / on-the-spot**	**No. of different stakeholders requesting support or providing content to EC3 / No. of active users on EC3 space**	**Extent to which EC3 (Europol) becomes the cybercrime information hub**

	assistance **No. of critical incident reporting from CERTs**	**Awareness among EU MS of critical incidents**	**Comprehensiveness of critical incident overview**
<u>R&D and TRAINING</u> **EU technical capacity for tackling cybercrime**	**No. of research projects developed/coordinated by EC3** **No. of requests (including on-the-spot) on technical and/or forensic issues made** **No. of training programmes supported by the EC3**	**No. of research projects resulting in tools for fighting cybercrime** **No. of support given on technical and/or forensic issues (incl. on-the-spot)** **No. of staff trained staff**	**Extent of use of new tools by MS and satisfaction rate** **Stakeholders' reliance on the 'helpdesk function' of the EC3** **Increase in volume ratio of trained staff over the total amount of staff**
Strategy	**Portfolio of EC3 strategic products delivered**	**Quality of strategic products (detail, scope, analytical method)**	**Extent to which EC3 strategic guidance is reflected at political level**
Outreach to stakeholders	**No. of contributions received from non-LE stakeholders / No. of collaborative projects between LE and third parties supported by EC3**	**No. of data exchanges/ No. of Memoranda of Understanding / No. of PPP agreements / No. of non-LE active users in EC3 Space**	**Extent to which MoUs and PPPs facilitated general EC3 work**

	No. of public awareness campaigns coordinated	**Delivery and dissemination of campaigns within the MS**	**Level of public awareness on cybercrime-related issues**

The EC3's work will be monitored, measured and evaluated to ensure the decision has achieved its intended objectives. To this end, the Commission will prepare an **evaluation report three years after the start of operations**, and send it to the European Parliament and to the Council for review. The report would be based on:

- ✓ an assessment of the results that will be published by the EC3 in its annual report, based on comprehensive objective data similar to those outlined above on performance indicators.
- ✓ any audit reports carried out by the Commission or on behalf of the Commission on the work of Europol, as well as any audits carried out by Europol itself.
- ✓ a survey of public and private stakeholders on their perceptions of the EC3's work in terms of supporting Member States' fight against cybercrime in general, technical capacity, research and training, outreach towards third parties, strategic direction and its role as a centre managing huge quantities of information flows.

The criteria that will be used to assess the effect and impact of the creation of the launch of the EC3 will be:

- ✓ progress made in the development of the EC3's activities
- ✓ success of the EC3's strategy in fighting cybercrime, in particular the extent to which each of the outcomes outlined in the Table of Indicators above materialise
- ✓ efficient and effective use of resources
- ✓ impact and implications for public and private stakeholders

The following will act as **the main monitoring indices**:

- ✓ high-profile and standard operations in cross-border cybercrime cases with actual suspects identified, arrested and prosecuted/victims identified
- ✓ accuracy/usefulness/timeliness of threat assessment reports and trend forecasts
- ✓ development of tools (including forensic) and their impact on law enforcement capability to detect and respond to cybercrime more effectively
- ✓ maintenance of databases and use of software tools for managing information flows
- ✓ quality and impact of strategies developed to anticipate and respond to threats

- ✓ quality of training (including the number of persons trained and the spread across the criminal justice landscape)
- ✓ quality and impact of platforms for collaborative action with third parties
- ✓ information exchange and data protection' (i.e. deficits, impacts, infringements, complaints, cooperation with the EDPS and MS, recommendations, etc)

Annex 1 — Comparison of Options according to six criteria

(source: RAND Europe, Feasibility study for a European Cybercrime Centre: Final report)

Comparison overview

Table 7.17 below provides an overview of how each of the feasible options compares in addressing the specific factors relating to the feasibility of establishing an ECC.

Table 7.17 Overall comparison of the options in addressing specific factors

	Maintain status quo	ECC owned by Europol	ECC hosted by Europol	Virtual ECC
Mandate	Serious and organised crime as per Art. 4(1) of the ECD Europol and Eurojust would be governed by existing arrangements which would evolve naturally (e.g. the revised Europol regulation) ENISA's activities in cybercrime would continue to evolve in the context of the new ENISA Regulation due 2012	Mandate would stem from existing Europol (serious and organised crime) governing instrument. ECD currently defines this as 'computer-related crime' and this is taken to include: hacking (AWF Cyborg); CEM (AWF Twins); credit card fraud (AWF Terminal), mass-marketing fraud Oversight of the ECC would be within Europol's existing arrangements (Europol Management Board; EP and Council)	This option would require a separate governing instrument Mandate might be different from that foreseen in current Europol governing instruments requiring further agreement and negotiation — however this would present complications in terms of the use of Europol's criminal intelligence gathering apparatus. Oversight would require new arrangements with the Council and Parliament	This option would require a separate governing instrument Mandate would need to be an amalgamation of those contained in the other agencies Bringing together a broader range of agencies might afford the possibility of a broader consideration of preventative measures with respect to cybersecurity
Resources	Resourcing is most closely tied to the strategy and mandate of the ECC No additional resources would be required save the annual year-on-year increase in resources for Europol	The level of resourcing would remain broadly similar as each other option (apart from the Do Nothing option) except for the source of the budget Could leverage existing Capex infrastructure on ICT platforms; Data Centre and SIENA.	The level of resourcing would remain broadly similar to each other option (apart from the Do Nothing option) except for the source of the budget Arrangements would need to be found (e.g. via service level agreements) to obtain use of Europol owned resources (e.g. data centre; SIENA)	The level of resourcing would remain broadly similar as each other option (apart from the option of maintaining the status quo) except for the source of the budget and a governance layer

Activities	Criminal intelligence and limited multi-source intelligence Operational support Training and education aimed at the law enforcement community	Criminal intelligence Operational support Broad training and capacity-building aimed at all members of the criminal justice community Coordination and cooperation (including fusion of non-criminal strategic intelligence)	Criminal intelligence Operational support Broad training and capacity-building aimed at all members of the criminal justice community Coordination and cooperation (including fusion of non-criminal strategic intelligence)	Criminal intelligence Operational support Broad training and capacity-building aimed at all members of the criminal justice community Coordination and cooperation (including fusion of non-criminal strategic intelligence)
Risks	Although the status quo option would not be exposed to any of the risks associated with the options involving the establishment of an ECC, the chief risk would be that activities continue to take place in a fragmented and piecemeal fashion leading to worse outcomes in tackling cybercrime	The risks under this option are that it might be difficult to establish effective governance of funding for an ECC since this would not be separate from Europol's overall budget	Institution within an institution would require complex governing instrument Complexity would also affect visibility by non-law enforcement stakeholders Recreating the complex data protection regime would be complex, further hindering immediate results	Perception that its not doing anything Institutional complexity (how to link each institution or tie them together) Poor visibility/acceptability by other stakeholders Recreating the complex data protection regime would be complex, further hindering immediate results
Cooperation	Existing fragmented and ad-hoc co-operation would continue	Would possibly require further amendments to the ECD (Article governing information exchange with non-law enforcement stakeholders) since as scoped this excludes deeper cooperation with private sector — at present Europol cooperation with the private sector is via liaison and limited to strategic cooperation because of data protection requirements	An ECC hosted at but not owned by Europol would be able to create deeper and more substantive cooperative links with the private sector than might be possible under the first option (due to the possibilities to tailor-make a specific governance structure to address this)	Opportunities for cooperation would be broader giving consideration to the existing relationships established by Europol (with the law enforcement and criminal justice community) and ENISA (with the national/governmental CERT community and the private sector)
Impacts	Impacts would continue to evolve from existing activities such as criminal intelligence analysis (more cases being solved) training (more law enforcement officers being trained) and those Member States collecting more data from a public reporting system	ECC within Europol would allow better cross fertilisation and linking between different crime types. The hosting of the ECC in Europol would be beneficial in future proofing cybercrime responses as being a facet of criminality rather than a specific and 'bounded' crime type in and of itself known as mainstreaming.	Whilst an ECC hosted by but not at Europol would have a focus on law enforcement impacts it would perhaps have more flexibility in consideration of other impacts (for example, prevention)	The impacts of a virtual ECC would be difficult to judge and separate out from those that might already occur under the status quo

Annex 2 — EC3 costs 2014 – 2020

For 2014: The foreseen budget for EC3 comes to €6.4M. An amount of €1.7M facilitates the additional staff resources (17 new posts). The remaining non-staff related budget of €4.7M will cover the main operational activities to be delivered (Data Fusion, Operations, Research & Development and Training, Strategy and Management). It includes the ongoing operational activities (missions, training, financial support for operational meetings, operational equipment, etc.), expansion of the existing building facilities for the lab, building a 24/7 command centre and ICT expenditure. A significant amount of €2.9M is planned for ICT investments (screens for the command centre, forensic software, laptops, workstations, network expansion, ICT support, service and licences).

2015 – 2020

Commitment appropriations in EUR million (to three decimal places)

Indicate objectives and outputs ⇩			Year **2015**		Year **2016**		Year **2017**		Year **2018**		Year **2019**		Year **2020**		**TOTAL**	
	Type[8]	Average cost	Number	Cost	Number	Cost	Number	Cost	Number	Cost	Number	Cost	Number	Cost	Total number	Total cost
SPECIFIC OBJECTIVE NO 4 Strengthen EU capacity to tackle cybercrime to avoid harm to EU citizens. businesses and losses to																

[8] Outputs are products and services to be supplied (e.g.: number of student exchanges financed, number of km of roads built, etc.).

the EU economy															
- Output	Supporting MS investigations to dismantle cybercrime networks operations	1.237	2	2.474	2	2.850	3	3.112	3	3.450	3	3.674	3	3.674	16	**19.234**
- Output	Information exchange between all stakeholders and fusion of data	0.516	4	2.063	5	2.375	5	2.594	6	2.875	6	3.063	6	3.063	32	**16.033**
- Output	Provide EU-wide strategic assessments. develop forensic tools. PPP. training	0.344	6	2.063	7	2.375	8	2.594	8	2.875	9	3.063	9	3.063	47	**16.033**
Subtotal for specific objective No 4				6.600		7.600		8.300		9.200		9.800		9.800		**51.300**