Feasibility study for a European Cybercrime Centre

Neil Robinson, Emma Disley, Dimitris Potoglou, Anais Reding, Deidre Culley, Maryse Penny, Maarten Botterman, Gwendolyn Carpenter, Colin Blackman and Jeremy Millard

Final report

TR-1218-EC

Prepared by RAND Europe

February 2012

Prepared for the European Commission, Directorate-General Home Affairs, Directorate Internal Security Unit A.2: Organised Crime

RAND EUROPE

Preface

This report was prepared for DG Home Affairs as the final report of the feasibility study into a European Cybercrime Centre (ECC).

The objectives of this study are broadly two-fold. The first aim is to collect data on the state of knowledge with regards to cybercrime: its extent, costs and implications as well as governmental responses (specifically in the area of law enforcement). The second aim, noting the conclusions of the Councils of 2008 and 2010 on Cybercrime and the European Union's Internal Security Strategy of 2010, is to evaluate the feasibility of the establishment of the ECC in relation to a number of factors including mandate, activities, resources, risks, co-ordination and impacts.

Given the broad scope of the study and need for a wide range of skills, RAND Europe formed an extended project team of researchers drawn from additional organisations, DTI and GNKS Consult and Colin Blackman. The study conducted systematic consultations with representatives of both national and European level law enforcement and criminal justice community. This report also includes input from others outside the criminal justice domain, who were consulted on an occasional basis.

RAND Europe is an independent not-for-profit policy research organisation that aims to improve policy- and decision-making in the public interest, through research and analysis. RAND Europe's clients include European governments, institutions, NGOs and firms with a need for rigorous, independent, multidisciplinary analysis.

For more information about RAND Europe or this document, please contact:

Neil Robinson, Research Leader

RAND Europe
Westbrook Centre
Milton Road
Cambridge CB4 1YG
United Kingdom
Tel: +44(0)7872691722
E-mail: neil_robinson@rand.org

This study has been carried out for the Directorate-General Home Affairs in the European Commission as result of the procurement procedure HOME/2010/ISEC/FC/059-A2 for an amount of € 169.400,00.

The report expresses the opinion of the contractor (consortium of Danish Technological Institute, RAND Europe Cambridge Ltd, ICEG European Research and Consulting Ltd and GNKS Consult BV) who performed the study. These views have not been adopted or in any way approved by the European Commission and should not be relied upon as a statement of the European Commission's or the Home Affairs DG's views. The European Commission does not guarantee the accuracy of the information given in the study, nor does it accept responsibility for any use made thereof.

European Commission

DG Home Affairs, Directorate A

Rue du Luxembourg 46

B-1049 Brussels

HOME-PROCUREMENT-A4@ec.europa.eu

Contents

List of tables

List of figures

Acknowledgements

We would like thank all those from the European and international law enforcement and criminal justice communities who contributed of their time to participate in this study including those from the European Cybercrime Task Force. In addition, we are especially grateful to the Council of Europe and Interpol in Lyon for giving of their time and arranging field visits. Finally, we would like to extend our thanks to Professor David Wall for his comments, our Quality Assurance Reviewers at RAND Europe and our Project Officer for their respective input throughout this study.

Executive summary

Background

Internet access is attended by criminal activities that exploit online transactions and the reach that the Internet affords

Cybercrime is an increasingly important concern for policy-makers, businesses and citizens alike. In many countries, societies have come to rely on cyberspace to do business, consume products and services or exchange information with others online. By 2011, nearly three quarters (73 percent) of European households had Internet access at home and in 2010 over third of EU citizens (36 percent) were banking online. Modes of connecting are growing ever more complex too. Smartphones can access high-speed data networks, enabling people to surf the Internet when on the move, and developments such as cloud computing are helping to realise the possibilities of limitless data storage.

The benefits of cyberspace are accompanied by a downside, however. 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, motivated not by money but by anger or ideology. Many cybercrimes target financial institutions or online entities where transactions take place (for example, the EU's own Emissions Trading Scheme). Still other types of cybercrime may focus on personal data. According to the Organisation for Economic Co-operation and Development (OECD), personal data has become the lifeblood of the Internet economy, so thieves know that by finding such data they can either sell it on or use it to target victims. Some types of cybercrime 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: online bullying or stalking via virtual communities such as Second Life have been documented.

Measurement of extent and costs of cybercrime remains a challenge, though EU agencies Europol and Eurojust are making progress in training and data infrastructure needed to make accurate assessments

It is difficult to estimate precisely the real extent or costs of cybercrime. Industry predictions are that it runs into the hundreds of millions of Euros per year. Official reports and criminal justice statistics paint a much different picture with small numbers of incidents. Regardless, the trends are that the phenomenon is increasing. Measurement is complicated by two factors. Firstly, separating true cybercrime from fraud is complex. Secondly, there are low levels of reporting. Citizens are confronted with myriad ways to report cybercrime. Businesses might be reluctant lest it affect their share price or cause reputational damage.

These activities have not gone ignored, however. At a European level, Europol, the EU's own criminal intelligence organisation, has had an emergent capability to address cybercrime for some time. Europol has strict data-protection arrangements in place, which means it can process personal data when supporting Member State operational investigations alongside the European Judicial Co-operation Unit (Eurojust). Europol is also driving training and best practice provision for addressing cybercrime, in conjunction with training partners such as the European Police College (CEPOL). In addition, Europol has an extensive infrastructure for collecting, analysing and processing sensitive criminal intelligence and investigative data.

Many Member States have a specialised law enforcement unit set up to address cybercrime. These units often conduct operational support activities and forensics, as well as providing training and sometimes working alongside the private sector. They can focus on different aspects or types of cybercrime; often they are under pressure from budgets and requests from other criminal investigations where their forensic capability is in demand.

Capability must be broadened and collaboration mechanisms strengthened to improve information-sharing and data collection, and expand expertise for complex cases

However, challenges remain. Not least is the uncertainty about the importance of reliable data and the pursuant need to establish better co-operation models between law enforcement agents and others, especially those in the private sector such as banks, communications providers and CERTs. There is also a need to broaden capability to ensure that specialised units can focus on the more complex or serious cases. Cybercriminals can leverage poor co-operation between different countries – this is especially true for those countries that "export" cybercrime.

With this in mind, policy-makers have taken considerable interest in identifying ways to improve the situation. In April 2010, the European Council discussed the possibility of a European Cybercrime Centre (ECC), to be set up by 2013, to build analytical and operational capacity to tackle cybercrime. The subsequent Internal Security Strategy foresaw that an ECC, established within existing structures, would thus act as Europe's focal point in the fight against cybercrime.

A European Cybercrime Centre could address many of the current challenges but requires careful assessment with respect to most suitable options in terms of feasibility, costs, mandate, risks and relationship to other organisations

In order to assess its feasibility, a consortium led by RAND Europe was asked by the European Commission to conduct a two-part study: firstly, to assess and evaluate the state of current efforts to deal with cybercrime, and, secondly, to consider the feasibility of an ECC across a range of different aspects such as mandate, resources, activities, risks, impact and interoperability with other organisations.

After considering a range of options, the study team looked at four in detail:

- Maintaining the status quo
- An ECC owned by Europol
- An ECC hosted but not owned by Europol
- A virtual ECC

Our conclusions were that an ECC should deploy resources in a targeted fashion. For example, expanding training efforts would help Member States in dealing with the broad range of frauds and crimes perpetrated with the aid of computers. Criminal intelligence efforts should be dedicated to addressing the most serious forms of cybercrime. There was limited difference in the resource implications across each option. Out of the four options we chose for specific consideration, there was limited difference in cost. However, there were major differences in institutional complexity and the organisational parameters between the different options. An ECC should continue to strengthen Europol's analytical capability for criminal intelligence and operational support, whilst facilitating new forms of collaborative working at the Member State level, between law enforcement and national/governmental CERTs.

The ECC should be run according to a model that places it in the middle of a broad capability to tackle cybercrime, exploiting the strengths of each organisation that possesses existing competencies, skills and knowledge. This does not necessarily mean seting up a wholly new organisation to deliver such a capability. Rather the feasibility of the ECC should be considered with respect to doing so with minimal organisational change. A European cybercrime capability would be at the disposal of the Member States and the ECC would be able to further support the work of the EUCTF.

We identified four sets of activities that the ECC should bring together in this capability based approach:

- Providing criminal intelligence analysis and operational support to Member State investigations, building upon the established track record and unique competencies of Europol and Eurojust.

- Broad based training, education and professional development for all members of the criminal justice community, by leveraging the role of CEPOL and the content and training legacy established by ECTEG. Such training would include primarily week long courses offered to help great a minimum baseline of familiarity with cybercrime and crimes where there is an IT aspect.

- Co-operation, collaboration and outreach with a broader set of non-criminal justice stakeholders including the private sector but specifically national/governmental CERTs through the establishment of joint CERT-LEA Liaison Officers co-funded from the ECC with the input of ENISA. In addition, we propose a European Cybercrime Resource Facility to act as a one stop shop for cybercrime knowledge exchange and best practice sharing. This co-operation and collaboration would help inform a much broader multi-source intelligence picture. In turn, through the work of a new Data Fusion Unit, this would allow a more strategic criminal intelligence analysis and operational support capacity.

- Facilitating a common, standards based reporting platform to support the sharing of cybercrime data, in a decentralised fashion, between members of the public and law enforcement, private industry (such as financial institutions and CERTs) and between law enforcement for cross border cases. Whilst the challenges of collaboration should not be underestimated a good first step would be to invest in a mechanism that allows the structured exchange of data. By analysing certain meta-elements the ECC could thereby build up a picture of trends and patterns which would inform further allocation of resources, intelligence and planning.

To estimate the resources required to perform these functions is no easy task. Regardless of expected level of workload for intelligence analysis and operational support, we estimate that three personnel would be required for the governance team, a further three for the European Cybercrime Resource Facility (ECRF) and one for the initial stages of the Data Fusion Unit (DFU). After the first year, during which we suggest a pilot of the Joint CERT-LEA Public Private Partnership (PPP) Network in three Member States, we envisage that it would be possible to discern a more precise idea of the likely resources needed to perform criminal intelligence analysis and operational support activities. Other resources would be needed to cover travel and subsistence for various meetings, an extensive expansion of the training and professional development programme and other associated activities. However, since all of the options under detailed consideration involved Europol (which has just opened its brand new facility in The Hague) few additional one off costs are envisaged.

The risks associated with an ECC revolved around its visibility and institutional complexity. Its impacts should be focused on measurable benefits for law enforcement rather than trying to tackle the much broader aspect of cybersecurity. Finally, an ECC would need to work with a range of partners from the public and private sector (particularly national/governmental CERTs) including not only those within Europe but also others such as Interpol and third countries.

Our final recommendation was that an ECC be set up within Europol.

We estimate that for the first (pilot) year between January and December 2013, a sum of €3.36 million Euros would be required. This would cover the personnel for the ECC governance team, ECRF, the pilot of the DFU and CERT-LEA PPP Pilot and expanded training provision, travel, other operational costs, plus the development of a standards based cybercrime reporting platform. Subsequently, this figure might rise (for example between €7 million and €42 million) if it seems that radically more criminal intelligence analysts and operational support personnel are required, due to the increased information flow coming into the DFU.

Considering impacts, we might envisage that the ECC could support in the handling of more cases, but also the achievement of more intangible (but no less important) impacts including better analysis of patterns, trends and data on the scale of the problem, smoother interaction between law enforcement and the private sector (especially the CERT community) importantly at the Member State but also the European level and enhanced co-operation with international stakeholders (such as Interpol and third countries). As well as bringing cybercriminals to justice, the ECC would no doubt work to make sure that Europe can fully benefit from the potential contribution of cyberspace to economic growth and society as safely as possible.

A staged approach is required based on clear principles

In conclusion, we base our recommendation and way forward around a number of key principles. It is important to recognise two main structural considerations – firstly, that the current climate of austerity weights heavily against new, expensive initiatives (such as the creation of a brand-new physical building to house an ECC) and, secondly, that without a wider information picture, it would be ineffectual to deploy further the resource of criminal intelligence analysts. We also note the importance of adopting a broad-based capability approach to addressing cybercrime, with the ECC at its heart, which would bring together existing efforts from some of the public and private organisations we have considered. The principles for implementation of an ECC include the following:

- The participation of Member States must be central to the efforts and impact of the ECC.
- The oversight and governance of the ECC must involve all key players including non-law enforcement partners.
- The principle of subsidiarity must govern the scope of the ECC's work.
- The ECC should be flexible in focusing its resources depending on the type of cybercrime.
- The ECC must operate with respect for data protection and fundamental human rights.
- Greater co-operation between law enforcement and the national/governmental CERT community will be crucial to the delivery of an improved cybercrime capability.
- The ECC must support a broad-based capability within Member States.
- The ECC must strengthen Europol's existing capability based on a broader information picture.
- The ECC should set up a common infrastructure for reporting between many different types of interested parties.
- Over the long term, the ECC should work to develop an improved common picture of the extent of the phenomena of cybercrime.

To achieve these high-level principles our proposed "pathfinder phase" in 2013 would lead to Full Operating Capability in 2014. In particular, the initial phases would put in place measures to inform more effective deployment of Europol's valuable sensitive criminal intelligence and operational support measures.

In the end, an ECC can bring together the strands of different organisational efforts to address cybercrime in a combined pan-European capability.

Glossary

ANSSI – Agence nationale de la sécurité des systèmes d'information (France)

APWG – Anti-Phishing Working Group

AS – Autonomous Systems

BGP – Border Gateway Protocol

BKA – Bundeskriminalamt (Federal Police, Germany)

BSI – Bundesamt für Sicherheit in der Informationstechnik (Federal Office for Information Security, Germany)

CAIDA – Co-operative Association for Internet Data Analysis

CATS – French acronym for the Article 36 Committee

CDN – Content Delivery Networks

CEOP – Child Exploitation and Online Protection Centre (UK)

CEPOL – European Police College

CERT – Computer Emergency Response Team

CFN – Computer Forensic Network

CIIP – Critical Information Infrastructure Protection

CIRCAMP – Cospol Internet Related Child Abusive Material Project

CNAIPIC - Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (Italy)

CNCPO – Centro nazionale per il contrasto alla pedo-pornografia su Internet (Italy)

CoE – Council of Europe

COSI – Standing Committee on Operational Co-operation on Internal Security

COSPOL – Comprehensive Operational Strategic Planning for the Police

CSES – Centre for Strategy and Evaluation Services (UK)

CSIRT – Computer Security Incident Response Team

CSOC – Cyber Security Operations Centre

CSP – Communications Service Provider

DDoS – Distributed Denial of Service

DFU – Data Fusion Unit

DJF – Economic and Financial Crime Division (Belgium)

DNSSEC – Domain Name System Security Extensions

DPA – Data Protection Authority

ECC – European Cybercrime Centre

ECCP – European Cybercrime Platform

ECN – European Cybercrime Network

ECTEG – European Cybercrime Training and Education Group

EECTF – European Electronic Crime Task Force

EFC – European Financial Coalition against Commercial Sexual Exploitation of Children Online

EGN – European Genocide Network

EISAS – European Information Sharing and Alerting System

EJN – European Judicial Network

EJTN – European Judicial Training Network

EMCDDA – European Monitoring Centre for Drugs and Drug Addiction

ENISA – European Network and Information Security Agency

ENU – Europol National Unit

EP3R – European Public–Private Partnership for Resilience

EPE – Europol Platform for Experts

EU ISEC Programme – Prevention of and Fight Against Crime

EUCTF – European Union Cybercrime Task Force

EUMS – European Union Member States

Eurojust – European Judicial Co-operation Unit

Europol – European Police Office

EWPOTC – European Working Party on Information Technology Crime

FOC – Full Operating Capacity

HaaS – Hardware as a Service

HTCC – High-Tech Crime Centre (Europol)

IANA – Internet Assigned Numbers Authority

IC3 – The Internet Crime Complaint Centre: a partnership between the Federal Bureau of Investigation (FBI), the National White Collar Crime Centre (NW3C), and the Bureau of Justice Assistance (BJA) (USA)

ICANN – Internet Corporation for Assigned Names and Numbers

ICROS – Internet Crime Reporting Online System

ICSPA – International Cyber Security Protection Alliance

ICT – Information and Computer Technology

IETF – Internet Engineering Task Force

IFOREX – Internet and Forensic Expert Forum

IGF – Internet Governance Forum

INHOPE – International Association of Internet Hotlines

IOC – Initial Operating Capacity

iOCTA – Threat Assessment on Internet-facilitated Organised Crime

IODEF – Incident Object Definition Exchange Format

IP – Internet Protocol

IPTV – Internet Protocol television

IP – Internet Protocol (a networking protocol for a system of addresses used to identify devices on a network)

IRC – Internet Relay Chat

ISP – Internet Service Provider

ITU – International Telecommunications Union

IWF – Internet Watch Foundation (UK)

IX- Internet eXchanges

JHA – Justice and Home Affairs Council

JIT – Joint Investigation Team

JSB – Joint Supervisory Board

KLPD – Korps landelijke politiediensten (National Police Services Agency, Holland)

LEA – Law Enforcement Agency

LIBE – Committee on Civil Liberties, Justice and Home Affairs

LINX – London Internet eXchange

LMS – Learning Management System

MAAWG – Messaging Anti-Abuse Working Group

MLAT – Mutual Legal Assistance Treaties

MMORG - Massively Multiplayer Online Role Playing Games

NAS – Network Attached Storage

NCSC – National Cyber Security Centre

NGO – Non-Governmental Organisation

NICC – National Infrastructure Co-ordination Centre (USA)

NICC – National Infrastructure against Cybercrime (Holland)

NIS – Network and Information Security

NIST – National Institute for Standards and Technology (USA)

OCLCTIC – Office Central de Lutte contra la Criminalité liée aux Technologies de l'Information et de la Communication (France)

OCSIA – Office of Cyber Security and Information Assurance (UK)

OECD – Organisation for Economic Co-operation and Development

PPP – Public–Private Partnership

RfC – Request for Comments

RIPE NCC – Réseaux IP Européens (European IP Networks) Network Co-ordination Centre

RIR – Regional Internet Registry

RTX Unit – Reitox [Réseau Européen d' Information sur les Drogues et les Toxicomanies] and international co-operation Unit (at the EMCDDA)

SCADA – Supervisory Control and Data Acquisition Systems

SIENA – Secure Information Exchange Network Application

SMTP – Simple Mail Transfer Protocol

SNS – Social Networking Site

SOCA – Serious Organised Crime Agency (UK)

UGC – User-Generated Content

VPN – Virtual Private Network

WSIS – World Summit on the Information Society

XML – eXtensible Markup Language

CHAPTER 1 Introduction: policy background and objectives of this study

In this chapter we lay out the various policy statements leading up to the articulation, at European level, of a European Cybercrime Centre (ECC). There has been concern from policy-makers that the growing reliance on cyberspace and the trust placed in it makes the need to address the risks ever more apparent. In particular, there is concern that the nature of cyberspace, which transcends geographical borders, combined with the pervasion of technology in everyday life, provides increased opportunities for crime to take place.

As Internet connectivity broadens and the means by which people participate in cyberspace proliferate, the scope for abuse widens. Such types of abuse may be highly complex and require different skills and capacities in the public and private sector to identify monitor and address. Given the levels of usage of the Internet, credit card transactions and take-up of e-Commerce, not to mention use of e-Government, there is concern at the policy level that the misuse of cyberspace may seek to threaten participation and take-up of such benefits, resulting in increasing mistrust of cyberspace.

1.1 Policy background to the ECC

Calls for the creation of a European Cybercrime Centre (ECC) can be traced in a number of recent decisions and policy statements from the Council. These articulate how EU-level support and facilitation could better aid Member State efforts to address cybercrime, especially as it would appear that the complexity and scale of the phenomena have, for some years, presented significant challenges for EUMS.

JHA Council Conclusions in 2008

In 2008 the Justice and Home Affairs Council (JHA) issued its Conclusions on Cybercrime,[1] inviting Europol to "establish and host a European platform which will be the point of convergence of national platforms and will have as its purpose to:

- Collect and centralise information about offences noted on the Internet, supplied by national platforms and first analysed by them to determine whether the offences are European or extra-national in nature and hence need to be notified to the European platform.

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

- Send the information concerning them back to national platforms and ensure ongoing mutual information exchange.
- Set up a European information website on cybercrime and disseminate information about the existence of national platforms.
- Draw up regular operational and statistical reports on the information collected."

Later that year, the Council issued Conclusions on a Concerted Work Strategy and Practical Measures Against Cybercrime.[2] These relate, firstly, to "short- and medium-term" measures, and, secondly, to only "medium-term" measures. Inter alia, they invited "Member States and the European Commission to investigate short- and medium-term measures concerning:

- Setting up a European platform aimed at reporting criminal acts committed on the Internet.
- Setting up national frameworks and exchanging best practice regarding cyber patrols, which is a modern tool against crime on the Internet, enabling information on nicknames to be shared on a European scale in accordance with domestic laws on the data exchange.
- Resorting to joint investigation and enquiry teams.
- Finding a solution to the problems caused by electronic networks roaming and by the anonymous character of prepaid telecommunication products."

These Council Conclusions invited Member States and the European Commission to "investigate in the medium term:

- Exchanging information on the mechanisms for blocking and/or closing down child pornography sites in Member States (MS). Service providers should be encouraged to adopt these measures. If necessary, the European platform could be a tool for establishing a common blacklist.
- Facilitating remote searches if provided for under national law, enabling investigation teams to have rapid access to information, with the agreement of the host country.
- Developing temporary definitions of categories of offences and statistical indicators to encourage the collection of comparable statistics on the various forms of cybercrime, taking into account the work that the European Union is presently doing in this field."

The Stockholm Programme

On 10–11 December 2009 the Council adopted the Stockholm Programme.[3] One aspect of the programme is to promote policies to ensure network and information security and

[2] JHA Council Conclusions 2987th JHA meeting (2008)

[3] The Stockholm Programme – An open and secure Europe serving and protecting citizens

faster EU reactions in the event of cyberattacks. It called, for instance, for both a modernised ENISA and an updated Directive on attacks against information systems.

Council Conclusions concerning an Action Plan to implement the concerted strategy to combat cybercrime April 2010

These initiatives were also reinforced by the Conclusions of the European Council in April 2010, which proposed actions in the short and medium term to specify how the main points of the concerted strategy should be implemented, most notably:

- Further investigation into perpetrators and the scale of the problem.
- Consolidation and revisions to the functions of the European Cybercrime Platform (ECCP) to facilitate collection; exchange and analysis of information (including via the Member States to set up national cybercrime reporting systems).
- Promotion of cross-border law enforcement co-operation and Public–Private Partnership (PPP).
- Continuation of existing activities such as the Cospol Internet Related Child Abusive Material Project (CIRCAMP).
- Promotion of the use of Joint Investigation Teams (JITs)

Over the medium term, the 2010 Council Conclusions asked for progress on the following:

- Ratification of the Council of Europe's Cybercrime Convention by the European Union.
- Raised standards of specialisation of police, judges, prosecutors and forensic staff in combination with Europol, the European Cybercrime Training and Education Group (ECTEG), Eurojust and the Commission.
- Encouragement of information sharing between MS law enforcement authorities (especially via the International Child Sexual Exploitation Database at Interpol).
- Assessment of the situation as regards the fight against cybercrime in the European Union and Member States.
- Adoption of a common, international approach to the fight against cybercrime (especially with regard to Domain Names and IP addresses)
- Harmonisation of the different 24/7 networks, reducing duplication.
- Promotion of relationships with other bodies both at European and International level on new technology subjects.
- Collation and updating of best practices on technological investigation techniques.
- Promotion and boosting of prevention activities including the use of networks using cyber patrols.

- Establishment of a documentation centre on cybercrime to serve as a permanent liaison body between users, victims' organisations and the private sector.

The April 2010 Conclusions also set out the broad terms for this feasibility study, requesting that the Commission consider creation of a centre to carry out evaluation and monitoring of preventative and investigative measures and the aforementioned actions (where they have not been achieved) and also to conduct other activities namely:

- Support the standards of education and practice across all parts of the criminal justice community (police, judges, prosecutors and forensic staff).
- Serve as a permanent liaison body between users, victims' organisations and the private sector (e.g. by considering a model European agreement for co-operation).
- Gather and update standards on best practice on technological investigation techniques with all members of the criminal justice community.
- Evaluate and streamline the use of computer investigation tools.
- Elaborate annual reports on cybercrime phenomena at European level and other problems relating to the use of new technologies and advise the Commission and the Council in further policy development.

The Internal Security Strategy 2010

Building on the Council Conclusions and the Stockholm Programme, the Commission stated in the EU Internal Security Strategy 2010[4]:

> 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 co-operation with international partners.

The aims of an ECC, as set out in this Communication are to:

- Improve evaluation and monitoring of existing preventive and investigative measures.
- Support the development of training and awareness-raising for law enforcement and judiciary.
- Establish co-operation with the European Network and Information Security Agency (ENISA) and interface with a network of national/governmental Computer Emergency Response Teams (CERTs).

The Communication states that an ECC should become the focal point in Europe's fight against cybercrime.

[4] European Commission, COM(2010) 673 final

Finally, at the operational level, the Harmony Policy Cycle has outlined strategic goals and operational action plans for criminal justice across the EU. Strategic goal 4 of this Cycle concerns the European Cybercrime Centre.

1.2 The objectives of this present study

Tasked by the Council in April 2011 and in line with the Commission's Internal Security Strategy adopted in November 2010, the Commission sought to verify the feasibility of establishing an ECC as a core element to improve both the prevention of and the fight against cybercrime and to raise overall security in cyberspace.

According to the Terms of Reference issued by the Commission[5], the purpose and scope of this study are to:

1. Identify and evaluate existing law enforcement and non-law enforcement methods in the Member States to report, process and handle cybercrimes, including whether the reporting of cybercrime is mandated by law in Member States.
2. Assess critically how and where a centralised analysis of cybercrime information at European level would be performed.
3. Take into account existing policy, legal and organisational frameworks currently governing the prevention of and fight against cybercrime in the Union (including the legal basis for measures and the costs of running these existing arrangements), and to consider new forms of cybercrime as they evolve.
4. Critically examine various possibilities of creating an ECC.
5. Illustrate the likely impact the establishment of an ECC will have on the future of cybercrime prevention and repression – including the cost of establishing and operating an ECC.
6. Arrive at clear recommendations for the preferred environment for an ECC: (a) the location (b) the tasks and legal issues (including integration into existing structure, set-up of a new entity).

It should be noted that the feasibility study is not formally an Impact Assessment, although it shares some features of that approach, for example in the manner in which the options are developed and assessed.

1.3 Structure of this report

In order to achieve these aims, we conducted a study that reviewed literature and documents relating to the phenomena of cybercrime, conducted interviews across a range of Member States, and ran a number of interactive consultations including a one-day

[5] Request for Services No HOME/2010/ISEC/FC/059-A2 on "Feasibility Study for the creation of a European Cybercrime Center" under DG INFSO Framework contract on "Provision of Impact Assessment and Evaluation related services" (SMART 2007/0035 – Lot 4)

scenario-based workshop held in Brussels in November 2011. This document is the final report of the study and its findings.

The remainder of this report is structured as follows:

- Chapter 2 sets out the findings so far from the literature review as to the definition of cybercrime and the available evidence as to its nature, prevalence and cost.
- Chapter 3 looks in detail at the relationship between cybercrime and cybersecurity.
- Chapter 4 sets out findings from interviews with heads of national specialist units responsible for dealing with cybercrime.
- Chapter 5 presents information on the four main EU-level organisations involved: Europol, Eurojust; CEPOL and ENISA.
- Chapter 6 describes the options that emerged from the literature review and Member State-level interviews.
- Chapter 7 conducts a comparison of the options.
- Chapter 8 provides a roadmap for implementation of these options.

PART I

CHAPTER 2 The understanding and measurement of cybercrime

2.1 Introduction

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. We begin this chapter with reference to examples of incidents, misuse and behaviour that is understood in practice to characterise cybercrime or fall within the scope of cybercrime. We next discuss various attempts (by academics, lawyers and policy-makers) to classify such activities into a framework or taxonomy. We then describe commonly accepted legal definitions that apply in the European Union by making reference to EU-level legal texts.

2.2 What is cybercrime?

In this subsection we describe in simple terms the following activities, which are commonly understood by practitioners to be types of cybercrime. Many of

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

In the sections below we qualitatively describe each type by reference to recent events and a straightforward understanding.

Malware and spam

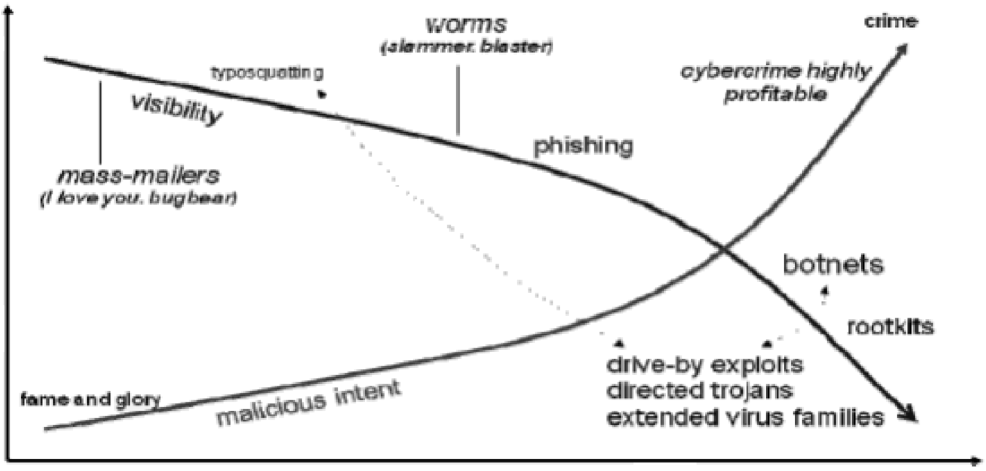
The term malware is used to summarise different forms of malevolent software that are designed to infiltrate and infect computers without the knowledge of the owner. Until recently, malware and spam could be considered as two separate issues. However, due to the emergence of botnets the two overlap to an increasing degree. (Botnets are networks of malware-infected computers, see below). Malware is often classified into "families" (related clusters of types of malware sharing characteristics) and "variant" malware (divergent versions of code in a particular family). Malware can be inserted into information systems by automated or manual installation.

Malware puts private and public sectors at risk because both rely on the value of information services. A response to malware (and spam) is complicated because malware not only incurs costs but also offers new business opportunities and revenue streams. Cost impacts include, but are not limited to, preventative measures, direct and indirect damages, remediation, infrastructure costs, and the opportunity costs of increased latency caused by network congestion. Business opportunities associated with malware and spam include anti-virus and anti-spam products, new and enhanced security services, and additional infrastructure investment in equipment and bandwidth (ITU, 2008).

Spam is defined as unsolicited, or "junk", e-mail sent by a third party. In addition to being an annoyance to users and administrators, spam is also a serious security concern because it can be used to deliver software Trojans, viruses, worms and phishing. Spam can also be used to deliver "drive-by downloads", which require no end-user interaction other than navigation to the URLs (web addresses) contained in the spam messages. Large volumes of spam could also cause loss of service or degradation in the performance of network resources and e-mail gateways (Symantec, 2010).

Figure 2.1 below illustrates how different types of malware may be understood on a continuum of malicious intent and visibility. Broadly speaking, as the malicious intent increases so does the technological complexity but the visibility of different types of malware decreases with its complexity.

Figure 2.1 Visibility of malware vs. malicious intent

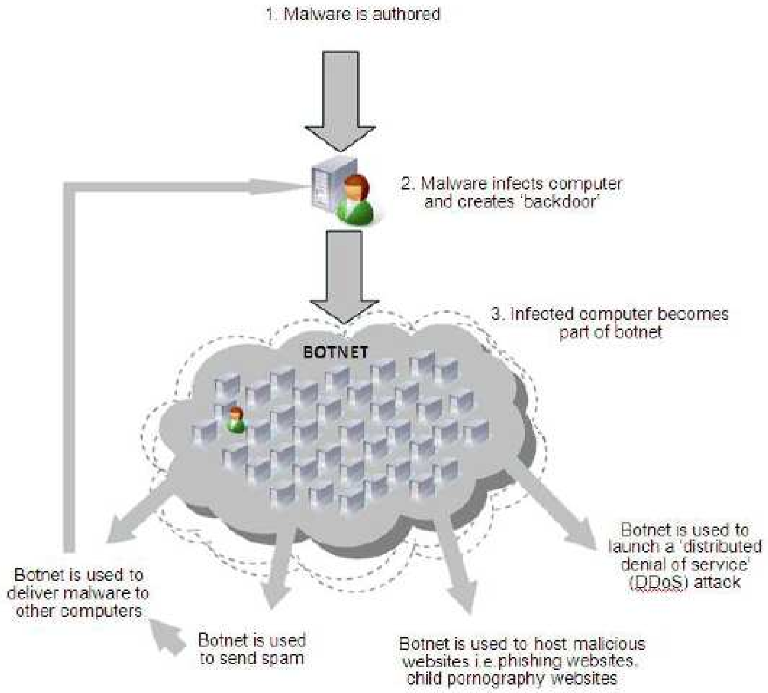


Source: www.govcert.nl

Botnets

Spam and malware are presently converging via the emergence of botnets. Botnets are programs that are covertly installed on a user's computer to allow an attacker to control the targeted computer remotely, through a communication channel such as Internet Relay Chat (IRC), peer-to-peer or HTTP. Botnets are very large numbers of remote-controlled malware-infected personal computers (Sommer and Brown, 2011). These machines are the origin of the majority of spam messages (van Eeten, M. *et al.* 2010) but they are also sustained and extended through spam (ITU, 2008). Around 80–90 percent of all spam is sent from machines infected with a botnet. Botnets are also used to host phishing campaigns often using forms of social engineering (manipulation) to trick users into revealing personal information. There are three principal types of actors involved in the illegal activities associated with botnets and their use: (1) malware authors, who write and release malicious code (2) bot-herders, who assemble and run the botnets, operating them through "command and control" channels, and (3) clients, who commission new malware development of botnet activity in order to accomplish fraudulent and criminal objectives such as spam distribution, identity theft, Distributed Denial of Service attacks, etc. Figure 2.2 outlines the range of functions carried out by botnets.

Figure 2.2 Initiation, growth and function of a botnet


1. Malware is authored
2. Malware infects computer and creates 'backdoor'
3. Infected computer becomes part of botnet
BOTNET
Botnet is used to deliver malware to other computers
Botnet is used to send spam
Botnet is used to host malicious websites i.e phishing websites, child pornography websites
Botnet is used to launch a 'distributed denial of service' (DDoS) attack

Source: OECD (2008)

As indicated above, botnets may be considered as a cybercrime "platform", which is a resource or crime service that can be adopted for a range of cybercrime purposes dependent upon different motivations (e.g. psychological, economic or political).

Distributed Denial of Service Attacks (DDoS)

This is another form of abuse that is based on the attack against a server or visible network end-point. The attack overwhelms Internet-connected systems and their networks by sending large quantities of network traffic to a specific machine. An attack from a single computer can be managed easily, so attackers use large numbers of compromised machines to carry out Distributed Denial of Service (DDoS) attacks (Sommer and Brown, 2011). Perpetrators must first take over the computers to be used for the attack, typically via e-mail or web-based malware. The attacker operates from a "command and control" computer that issues commands to these compromised machines. Often the immediate "command and control" computer has been compromised and is being remotely controlled from elsewhere. Popular targets include online gambling and e-commerce sites. A variant compromises the victim's machine and then denies the victim access to their own digital data, resources or other services (ITU, 2008). The user must pay a ransom in order to be able to unscramble their encrypted data. Businesses may run into substantial financial losses if their revenue-generating opportunities are affected or even come to a standstill, whether they give the extorted money or not.

Attacks against critical infrastructures

Attacks affecting the integrity of data or information systems used in Supervisory Control and Data Acquisition Systems (SCADA) could be used to overload power grids, block communications and financial transfers, etc. It has been reported that electronic threats, vulnerabilities and attacks are a reality for owner-operators of critical infrastructure, as documented in the report of the Centre for Strategic and International Studies commissioned by McAffee (Beker *et al.*, 2010). The data in this report comes from interviews with 200 industry executives from critical infrastructure enterprises in 14 countries. Eighty percent of the participants had faced a large-scale DDoS attack, and 85 percent had experienced network infiltrations (Beker *et al.*, 2010).

Stuxnet is the foremost example of an attack against critical infrastructure. Stuxnet is a sophisticated form of malware that operates by exploiting a number of vulnerabilities on Microsoft Windows. Stuxnet targets a specific Siemens SCADA program. If this program is running, Stuxnet looks for a particular configuration of industrial equipment and then launches an attack designed to manipulate certain microcontrollers to perform erratically while reporting normal functioning to operators of this system. Stuxnet was aimed at infiltrating Iran's heavily protected Natanz facility for enriching uranium. The delicate centrifuges at Natanz are crucial for Iran's nuclear weapons program, and they have suffered numerous unexplained failures since Stuxnet was launched. Since cyberspace pervades other critical infrastructures – not designed with cybersecurity in mind (such as electricity and transportation), experts point out it may not be too long before the same type of attack is tried out elsewhere.

Hacking

Hacking is a term with multiple meanings. It can refer to testing and exploring computer systems; highly skilled computer programming; the practice of accessing and altering other people's computers; or unauthorised copying of information such as personal data, intellectual property or trade or business secrets. Hacking may be carried out with honest aims or criminal intent. When related to cybercrime, hacking refers to the practice of illegally accessing, controlling or damaging other people's computer systems. Hacking can also include website defacement (i.e. files on websites may be changed or altered by unauthorised users). This type of hacking has been used most popularly to perpetrate politically or ideologically motivated messages. Other types of hacking may be focused on the theft of personal data, usually from poorly secured customer databases. A hacker may use their own technical knowledge or may employ any of the cybercrime tools and techniques listed above such as malicious software, botnets, etc (Commonwealth Australia, 2010).

Attacks may also involve large-scale Distributed Denial of Service (DDoS). Such examples include YLE Finland's public broadcaster and Britain's *Daily Telegraph*. Some forms of cyberattack have affected defence and aerospace companies, such as Lockheed Martin, the US defence contractor. Lockheed Martin revealed recently revealed that it had been the subject of a "significant and tenacious" cyberattack supposedly perpetrated via a vulnerability in the RSA SecureID "two-factor" authentication system used by employees to gain access to the corporate network (*The Economist*, 2007).

In the US, the Department of Defence (DoD) has been a favourite cyberspace target for decades. For example, in 1998, when the "Solar Sunrise" computer attacks were launched against the DoD classified computer network. In early 2011, UK Secretary of State for Defence Dr Liam Fox reported that the Ministry of Defence (MoD) was subject to "significant and intense" forms of cyberattack on a daily basis. He said that Britain was now in contact with an invisible enemy and that last year the MoD detected and disrupted more than 1,000 potentially serious attempts to breach its computer systems. Also in 2011, the US Federal Aviation Administration (FAA) was attacked, putting sensitive personal data of present and past employees at risk. The FAA commented that at no time was any air traffic control network at risk.

Other attacks target personal data, the "lifeblood" of the Internet economy. In April 2011 Sony's Playstation Network was attacked and the personal information of its users stolen. It is believed to be the largest data loss so far with over 77 million accounts compromised. Subsequently, in what might be considered as an example of cybercriminals switching their attention to another vulnerable target following the disclosure, the Sony Online Entertainment network was attacked, affecting 24 million customer records.

Scams and online frauds

Online scams include: online dating scams, where victims hand over money to fraudulent participants on dating websites; advance-fee scams where the victim is promised large returns on an upfront payment; and fake lottery, ticketing or online shopping scams, where victims are fooled into paying for a nonexistent product. Perpetrators may use other cybercrime tools to fashion and disseminate online scams (e.g. spyware or spam e-mail) (Commonwealth Australia, 2010).

Phishing

Phishing is an attempt by a third party to solicit confidential information from an individual, group or organisation by mimicking (or spoofing) a specific brand, usually one that is well known, often for financial gain. Phishers attempt to trick users into disclosing personal data, such as credit card numbers, online banking credentials and other sensitive information, which they may then use to commit fraudulent acts (Symantec, 2010). Users are misdirected to fraudulent websites (often hosted on botnets) that impersonate banks and acquire account details and passwords. This is one of the characteristics that distinguish phishing (e.g. the "Nigerian 419 scam" and other social engineering scams) from spam-based scams. Money can be moved out of accounts via dupes known as "money mules" that make it harder for the destination of funds to be identified. Fraudsters also use stolen personal information to apply for and exhaust credit cards and loans.

Identity theft and identity fraud

Identity theft is the assumption of the identity of another person, living or dead, irrespective of the motivation underlying this course of action. For example, taking on the identity of a dead person and living life as them, having abandoned one's own identity. By contrast, identity fraud is the transient or partial assumption of another's identity (Garlik, 2009). The risks from identity theft and identity-related fraud have become particularly apparent recently because of the prevalence of identity-related information used by many different types of organisations (banks, social networking sites, etc).

Advance-fee fraud conducted over the Internet

Financial fraud and identity theft are closely related, since the misuse of a stolen identity can be used for financial gain. However, it is worth noting that not every instance of identity theft relates to a financial fraud, since stolen identities can be used for many different purposes. Online financial fraud can also be achieved with false credit card information and some limited identity information, but not necessarily enough to assume the victim's identity fully (Garlik, 2009).

Online harassment

This type of cybercrime involves the use of computer to cause personal harm such as anxiety, distress or psychological harm, including abusive, threatening or hateful e-mails and messages and the posting of derogatory information online. There is not a single definition of "online harassment" or "cyberstalking" (Garlik, 2009). The terms are often used interchangeably. A simple definition of cyberstalking used in the Garlik report is: "the use of electronic communications including pagers, mobile 'phones, e-mails and the Internet to bully, threaten, harass and intimidate a victim". Online harassment can be seen as an element of cyberstalking, which has the additional factor of pursuit via electronic means: The distinction between harassment and cyberstalking is that cyberstalking is characterised by pursuit and fear (Garlik, 2009).

Production, distribution and downloading of child abuse material

This category of cybercrime covers a range of conduct that has an objectively ascertainable sexual element of harm to children.[6] It is somewhat different than the other forms of crime described since it represents activity with a more clearly discernible aspect of crimes against the person. According to international standards, this conduct can include the possession of and access to (where this access was deliberate and not inadvertent) images recording the sexual abuse of children by adults, images of children involved in sexually explicit conduct or of sexual organs where such images are produced and used mainly for sexual purposes with or without the child's knowledge. The ability to obtain access and store such images or content has been facilitated by the ubiquity of communications networks and by technological advances associated with digital technology including cheap digital cameras and low-cost digital storage. The UK has developed a set of image levels (1–5) describing the levels of seriousness of child sexual abuse images (Sentencing Guidelines Council Secretariat, 2007).

From a pragmatic perspective, this area of cybercrime can be classified into three components: production (creation of material), distribution (uploading and dissemination

[6] Paedophilic activity such as grooming a child online for sexual activity comes under what might be broadly understood as a misuse of communications since it is a separate preparatory activity.

of material) and downloading of material. There has been variable research into the links between those who acquire and download child abuse material from the Internet and those who produce it; and the relationship between online sexual exploitation of children and physical contact and abuse (e.g. see (Bourke, 2009). Further research has analysed the type and nature of victims (Qualye, 2011) and the channels of distribution (Mitchell, 2011), which noted from a nationally representative study in the USA that although the numbers of arrests for crimes relating to Internet-facilitated commercial sexual exploitation of children is "…relatively small, the victims of these crimes are a high-risk subgroup of youth and the offenders that try to profit from these crimes are particularly concerning from a child welfare perspective" (Mitchell, 2011).

Qualye (Qualye. 2011) randomly selected images from CEOP's ChildBase database and conducted further analysis of frequencies and cross-tabulations to discover that the odds of abuse images being female (rather than male) were about 4 to 1. Furthermore the odds of images being white (versus non-white) were 10 to 1. A significant gender difference was also identified across all age ranges of the distribution of children within the images.

Some producers and distributors may be only motivated by financial gain and not by personal sexual interest in children. A 2010 report from the European Financial Coalition (EFC) against Commercial Sexual Exploitation of Children Online noted that there appeared to be a decreasing number of commercial child abuse sites identified and that the distribution and downloading of material had appeared to move underground where access to networks was based on a reputational or peer-based rating system (i.e. access being granted on the basis of the production and dissemination of material by the consumer) (European Financial Coalition against Commercial Sexual Exploitation of Children Online, 2010) . The Annual reports of the UK Internet Watch Foundation (IWF) provide further insight into these phenomena. The IWF report for 2010 notes that online presence of these criminal images now has an average lifespan of 12 days, irrespective of the location of such images in the world (Internet Watch Foundation, 2010). This report further indicates that out of the 300 branded "sources" of commercial child sexual abuse websites that were active in 2010, the ten most prolific account for at least half of the commercial web pages it has seen.

However, this is not to say that commercial child abuse websites is the single defining characteristic of this phenomena. There would appear to be an increasing non-commercial aspect, where a variety of motivating factors drive individuals to share such images for personal gain.

Virtual cybercrimes

There are also types of cybercrime that only occur in cyberspace or on virtual networks. These include the "theft" or defrauding of virtual currency or possessions (e.g. from Massively Multiplayer Online Role Playing Games, MMORPG, such as *World of Warcraft*). In this instance the integrity of the servers that operate such virtual worlds may be affected or hacked, causing resources won or awarded to one player to be "stolen". Other similar types of cybercrime that exist solely within virtual worlds or networks include cyberbullying and cybertstalking (where a participant in a virtual world or game may be stalked or harassed by a fellow player).

Classifications of cybercrime

Some academics have devised alternative means of classifying these activities into cybercrime definitions, in order to bring some analytical order. Most of these have elements consistent with the distinctions made in the 2001 Budapest Cybercrime Convention (described below), in that they use the criterion of whether the computer (or information system) was the tool or the target. Some of the classifications distinguish between the offence being violent, non-violent or a property offence. This may be interesting in trying to apply classical definitions of crimes (e.g. against the person) to new types of misuse. Similarly, the consideration of forms of cybercrime being those that exist only in cyberspace (such as cyberstalking or the theft of "virtual" currency) raise interesting academic questions, but so far cyberbullying appears to be of limited interest to law enforcement. Ironically, it is these forms of misuse that are only visible from within cyberspace that perhaps, in one sense, might be considered as "pure" forms of cybercrime.

Some of the alternative classification systems encountered in our literature review are set out below in Box 2.1 and Figure 2.3.

Box 2.1 Meta overview of academic classification systems

Cross (2008) divides cybercrime into: white-collar, non-violent, and violent or potentially violent.

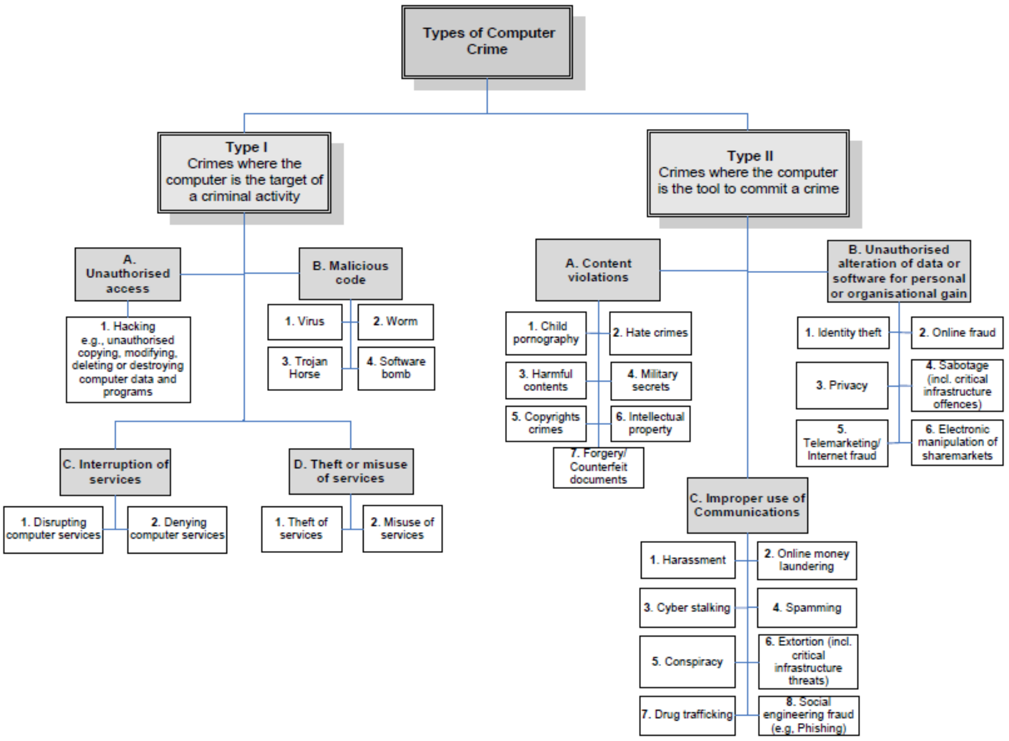
- White-collar can be divided into subcategories including cybertrespass, cybertheft, destructive cybercrimes and cyber or online frauds.
- Non-violent crimes use the Internet to accomplish criminal acts including Internet gambling, Internet drug sales, cyberlaundering (using electronic transfers of funds to launder illegally obtained money), and advertising/soliciting of prostitution services.
- Violent or potentially violent crimes that use computer networks can pose a physical danger to people including cyberterrorism, assault by threat, cyberstalking, online harassment and child pornography.

Wall (2001) classifies cybercrime into:

- cybertrespass, cyberdeceptions and thefts – stealing
- cyberpornography
- cyberviolence – doing psychological harm.

Yar (2006) classifies cybercrime according to the object or target of the offence e.g. crimes against property, crimes against morality, crimes against the person and crimes against the state.

Figure 2.3 Cybercrime classification from Alkaabi *et al.*

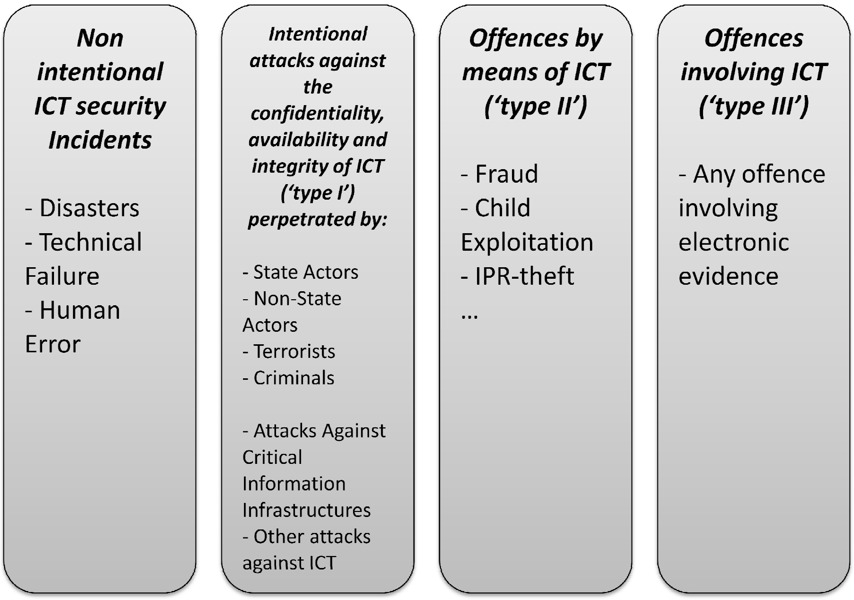

Types of Computer Crime
Type I Crimes where the computer is the target of a criminal activity
Type II Crimes where the computer is the tool to commit a crime
A. Unauthorised access
1. Hacking e.g., unauthorised copying, modifying, deleting or destroying computer data and programs
B. Malicious code
1. Virus
2. Worm
3. Trojan Horse
4. Software bomb
C. Interruption of services
1. Disrupting computer services
2. Denying computer services
D. Theft or misuse of services
1. Theft of services
2. Misuse of services
A. Content violations
1. Child pornography
2. Hate crimes
3. Harmful contents
4. Military secrets
5. Copyrights crimes
6. Intellectual property
7. Forgery/ Counterfeit documents
B. Unauthorised alteration of data or software for personal or organisational gain
1. Identity theft
2. Online fraud
3. Privacy
4. Sabotage (incl. critical infrastructure offences)
5. Telemarketing/ Internet fraud
6. Electronic manipulation of sharemarkets
C. Improper use of Communications
1. Harassment
2. Online money laundering
3. Cyber stalking
4. Spamming
5. Conspiracy
6. Extortion (incl. critical infrastructure threats)
7. Drug trafficking
8. Social engineering fraud (e.g. Phishing)

Source: Adapted from Alkaabi *et al.* (2010)

Alkaabi's typology above is undoubtedly comprehensive, describing the multitudes and nuances of computer crime. It splits type of computer crime using a criteria of whether the computer is the target/tool in addition to including types of misuse relating to the improper use of communications (a somewhat complex area in an international context, given widespread cultural differences as to what constitutes 'improper behaviour online'. However, it is also worth noting that this hierarchical model somewhat simplifies the complexity that some forms of misuse can include both types.

Representatives from the Council of Europe (see below) have also informally presented the 'cybercrime definitions' used in the Budapest Convention (see below) into the following simplified high level groupings:

Figure 2.4 Council of Europe based informal characterisation


Non intentional ICT security Incidents
- Disasters
- Technical Failure
- Human Error
Intentional attacks against the confidentiality, availability and integrity of ICT ('type I') perpetrated by:
- State Actors
- Non-State Actors
- Terrorists
- Criminals
- Attacks Against Critical Information Infrastructures
- Other attacks against ICT
Offences by means of ICT ('type II')
- Fraud
- Child Exploitation
- IPR-theft
...
Offences involving ICT ('type III')
- Any offence involving electronic evidence

Adapted from presentation given at the Octopus Conference of the Council of Europe Convention Against Cybercrime 21-23 November 2011, Strasbourg

This approach, although neither formal nor legally binding, is useful in its simplicity and the clarity with which it conceptually separates the specific forms of technical misuse from a broader set of crimes involving technology or having a technological aspect to them. However, this framework goes rather beyond a criminal definition since it also includes systematic errors, disasters, etc.

In any respect, there are some important characteristics that can be extracted from these different approaches:

- The sheer complexity in seeking to understand what can be defined as a preparatory act and the crime.
- The complexity of separating out incidents and attack vectors (Trojans; viruses) from motive (e.g. fraud).
- A separation between the computer as facilitating the crime, or being a source of evidence, and the computer or information system being the target.

As we further explore below, this last element will prove to be of most interest as the opportunity for attacks against information systems is most directly linked to poor levels of cybersecurity. In one sense it may be said that the root cause of these three types is different: cybercrimes where the computer or information system is the target arise because of poor levels of cybersecurity whereas other types of cybercrime occur because of society's increasing dependency upon technology.

2.3 Cybercrime legislation

In this section, we summarise the main legal frameworks of relevance to prosecuting and sanctioning the types of activity commonly regarded as cybercrime, described above.

The Council of Europe Convention on Cybercrime

For the purposes of this feasibility study, our starting point is the definition provided in the 2001 Council of Europe Convention of Cyber Crime (also known as the Budapest Convention and the Cybercrime Convention). This includes the following within a definition of cybercrime:

- **Core computer-related offences**, including "offences against the confidentiality, integrity and availability of computer data and systems" (informally: "type I").
- **Other computer-related offences,** in which "computer and telecommunication systems are used as a means to attack certain legal interests which mostly are protected already by criminal law against attacks using traditional means" (informally: "type II").
- **Content-related offences** of unlawful production or distribution of child pornography.
- **Offences related to infringements of copyright and related rights** – included separately because copyright infringements are one of the most widespread forms of computer- or computer-related crime.

The 2005 Framework Decision on Attacks Against Information Systems

In 2005 the Framework Decision on Attacks against Information Systems (2005/222/JHA) was released. Broadly, this document sought to approximate, into European law, the Council of Europe Budapest Convention on Cybercrime.

The objective of the Framework Decision on Attacks Against Information Systems is to improve co-operation between judicial and other competent authorities, via approximation of different Member State criminal law concerning what is now known as cybercrime.

Definitions of cybercrime between the Convention on Cybercrime and the Framework Decision are comparable to a great extent. Three central criminal offences are defined in the Framework Decision:

- Illegal access to information systems (article 2)
- Illegal system interference (article 3)
- Illegal data interference (article 4).

Under the 2005 Framework Decision, Member States had to make provision in national laws, within 2 years, for such offences to be punished, and the criminal act was defined as having to be intentional. Punishment was required for instigating, aiding, abetting and attempting to commit any of the offences listed.

In 2008 a report on the implementation of 2005/222/JHA was released by the European Commission.[7] It concluded that a "relatively satisfying degree of implementation" had been achieved despite the fact that transposition of the Framework Decision was still not complete. The European Commission invited those seven Member States that, at the time, had not yet communicated their transposition (brought into applicable national law) of the Framework Decision to resolve the issue.[8] Every Member State was asked to review their legislation to better suppress attacks against information systems and the Commission also indicated that given the evolution of cybercrime it was considering new measures as well as promoting the use of the Council of Europe and Group of 8 Nations (G8) network of contact points to react rapidly to threats involving advanced technology.

The draft Directive on Attacks against Information Systems

It is expected that the Framework Decision on Attacks against Information Systems 2005/222/JHA will be repealed and replaced by a new Directive on Attacks against Information Systems[9], which intends to provide closer harmonisation of the definitions and penalties related to certain types of crimes, and focuses on newer types of cybercrime, such as the use of botnets as an aggravating circumstance. Additionally, the Directive also aims to strengthen the existing structure of 24/7 national contact points, which should improve and facilitate cross-border communication.

In June 2011 it was reported that the European Council reached a general approach on the compromise text of the proposed Directive. All EU Member States, with the exception of Denmark, agreed with this approach. The Directive also refers to "tools" that can be used in order to commit the crimes listed in the Directive. Examples of such tools include malicious software types that might be used to create botnets. If the offences are against a "significant" number of computers or affect critical infrastructure then the Directive establishes a minimum sentence of five years.

The 2011 Directive on Combating the Sexual Abuse and Sexual Exploitation of Children, and Child Pornography

In late December 2011, a Directive approximating the Council of Europe Convention No. 201 was brought into force by the EU. The Directive harmonises around twenty relevant criminal offences at the same time as setting a high standard of penalties. The new rules must be transposed into national law within two years and include provisions to fight online child pornography and sex tourism. The directive also includes provisions to prevent convicted paedophiles moving between EU Member States from conducting professional activities involving regular contact with children. Measures to protect the child during investigations and legal proceedings are also included.

[7] European Commission Report COM (2008) 448

[8] Malta, Poland Slovakia and Spain did not respond to the request for information and the answers from Ireland, Greece and the United Kingdom were deemed as not possible to allow a review of their level of implementation.

[9] For the current draft, see Council of the European Union, 24/2/2005

Cybercrime law in EU Member States

Valeri *et al.* (2005) present a snapshot of the state of legislative frameworks governing computer and network misuse in EU countries in 2005. It can be seen that there was a wide variance in how certain accepted forms of computer and network misuse were penalised and the level of punishments available. For example, in some countries (at that time) certain types of offences were not even illegal whilst for others up to twelve different laws could be used to prosecute such incidents, with varying degrees of sanction including fine and imprisonment.

2.4 What can we draw from these different definitions and classifications?

Although these definitions vary in the offences included and the system of categorisation, they do indicate the kind of activities or misuse which can be thought of as cybercrime and they highlight the important distinction between crimes against computers or information networks (which is the core of cybercrime according to the Cybercrime Convention) and offences where Information Communications Technology (ICT) is used to perpetrate a "traditional" form of crime as "computer-mediated" crimes.

Throughout this discussion on the definition of cybercrime, however, it is important to remember that cybercrime has become familiar to EU citizens through the media. In the public consciousness, perceptions of the term "cybercrime" cover both crimes targeting computers and information systems and computer-mediated crimes. Cybercrime is understood by individuals to include well-known activities such as phishing, Distributed Denial of Service (DDoS) attacks, online child pornography, online identity theft and Nigerian 419 scams, as well as online fraud. This has important implications for how awareness campaigns are conducted and in terms of communication about reporting incidents.

There is also the issue of distinguishing cybercrime from other forms of activity that may affect cybersecurity. Examples include cyberterrorism or cyberwarfare. For example, Klimburg and Tirmaa-Klaar (2011) present some definitions of these concepts.

They note that cyberwar is a loaded term and has become highly popularised of late. Examples of cyberwar noted by Klimburg and Tirmaa-Klaar point to the 2007 attacks on Estonia and the 2008 attacks on Georgia. At the end of 2011, news came to light that the United States Department of Defence was authorised by Congress to deploy offensive cyberwar capability (Singel, 2011). Policy-makers have avoided using this laden term (since the term "war" implies specific consequences) preferring instead to frame the debate in terms of cyberdefence or cyberattack. Generally, although no strict legal definition has yet to emerge, the term refers to existing or potential nation-state directed cyberattack(s).

Defining cyberterrorism is even harder. Cyberterrorism appears to be a term in rather broader use in the United States, with both the Federal Bureau of Investigation (FBI) and the US Army proposing definitions. The US Army definition is split into two, either:

> "activities carried out in support of conventional terrorism" (e.g. "content", such as propaganda, recruitment, or planning)

> or actual "cyberattacks for terrorist purposes". (US Army, 2005)

Attempts to define cyberterrorism may run into similar complexities as with a traditional definition of terrorism, since it is highly subjective. A too-broad definition risks including a range of behaviour that may be politically motivated but not necessarily terrorist in nature in a democratic society. This may open up complex freedom of expression, privacy and human rights issues.

One European example of this was the Southern Tyrol Liberation Committee attacks on a number of Italian electricity pylons, which led to wide-scale disruptions of services (Schmid and Jongman, 2005). Another example is the cyberattacks by the "Anonymous" group against those companies that had boycotted or removed their support for the Wikileaks organisation (for example, Paypal and Amazon) following the arrest of Julian Assange.

In general an understanding is developing of a distinction between terrorism and nuisance attacks through the assessment of the amount of damage caused (or likely to be caused). This has lead to attempts to clarify and define "hacktivism" or "cybervandalism". The implication of this definitional confusion is not just academic because the technological signature of cyberattacks, whether perpetrated by criminals, national states or armed forces (the problem of attribution) confounds responses from governments that have different structures for dealing with crime, espionage or national defence.

2.5 Measuring cybercrime

Cybercrime appears to be a rapidly growing area of scholarly and policy interest, but the nature of this type of crime creates many unique challenges for collecting reliable statistics on its scale. For example, Florencio and Herley (2011) discuss the ways in which surveys on cybercrime are likely to produce a distorted and inaccurate picture of the prevalence of these offences.

In this section we look at some of the reasons why cybercrime is under-reported. With this under-reporting in mind, we review the available estimates of the prevalence and cost of cybercrime from a range of sources.

Why is cyber crime under-reported?

Data about different types of crimes and the criminal justice system have been collected for many years in several Member States to enable policy-makers, academics and others to examine crime trends and the functioning of criminal justice systems (Hunt *et al.*, 2011). This data includes:

- Reports to law enforcement authorities from individuals, businesses or organisations who believe they have been a victim of a crime.
- Reports to law enforcement from people who have witnessed a crime against someone else.
- Crimes that have come to the attention of law enforcement authorities independently of victim or witness reports – for example, during the investigation

of other offences reported by the public or perhaps via other law enforcement agencies.

- Crimes that come to the attention of organisations monitoring the Internet or e-mail traffic for cybercrimes.

Cybercrimes, however, often do not appear in these statistics and some of the reasons for this are explored in this section.

Members of the public do not report cybercrimes to the police or other national authorities

It might be the case that members of the public are not accustomed to reporting cybercrime to law enforcement organisations because events on the Internet are perceived to be outside the jurisdiction of the local police agency (Ferwerda *et al.*, 2010).

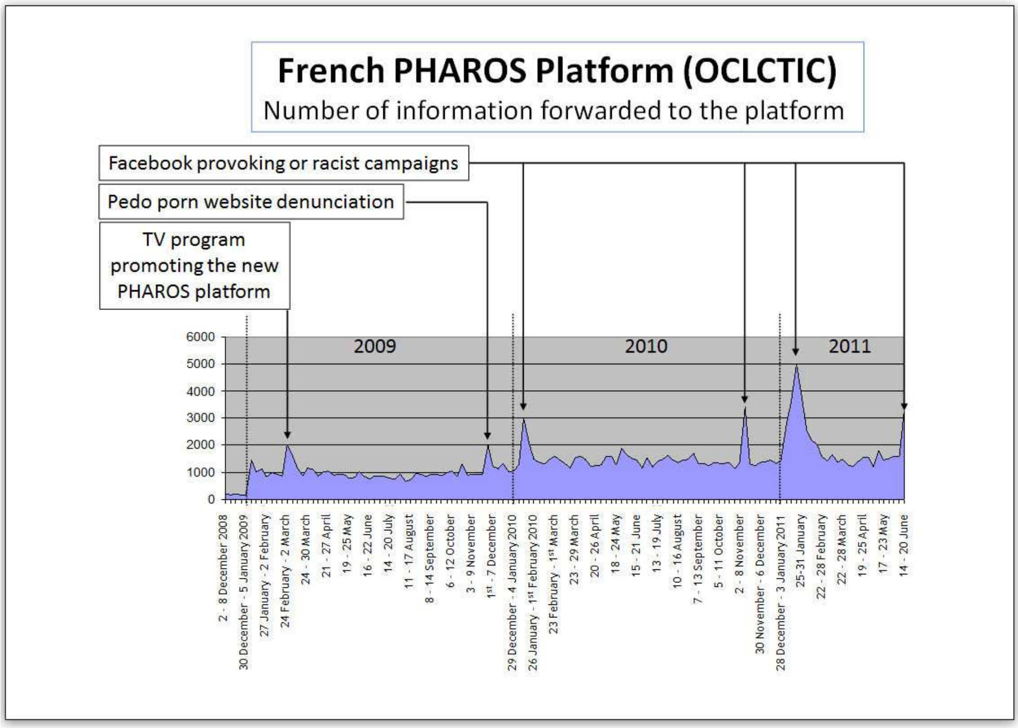
Many cybercriminals engage in scams that enable them to steal small amounts of money from a large number of individuals. This might discourage reporting in two ways: firstly, the small amount of losses suffered by each person may provide little incentive for reporting the incident; secondly, victims may frequently believe that the perpetrators cannot be easily identified and therefore there is little point in reporting the offence (United Nations Office on Drugs Crime, 2010).

There is also the question of the supporting infrastructure that might facilitate reporting. For example, currently in many countries victims must report crime by attendance at a police station. Although services such as emergency numbers exist to allow rapid alerts to law enforcement of a possible incident, very often (in some countries) in-person reporting is the only route through which a crime reference number can be obtained (which is needed for insurance purposes).

It is possible to discern a degree of fragmentation of reporting mechanisms. From the perspective of the citizen, he or she may have a number of routes to reporting cybercrime. Consider the instance of a phishing attack. In this case, the affected citizen might choose to alert the banking institution but they could also have the choice of their ISP, local police, or even an NGO.

The chart below, from a presentation given by the Assistant Head of the Office Central de Lutte contra la Criminalité liée aux Technologies de l'Information et de la Communication (OCLCTIC) in France shows data from the Pharos reporting platform. This platform receives 1,500 reports per day of suspicious websites or messages that members of the public encounter during Internet surfing. This chart is instructive in displaying the relationship between popular media and reporting, as well as a slight increase in reports between 2009 and 2011.

Figure 2.5 Number of reports issued to Pharos 2009–2011



Source: Paget (2011)

Businesses and corporations do not report cybercrime to the police or other national authorities

The private sector has made and continues to make attempts at gathering and analysing cybercrime statistics (Baker *et al.*, 2011; McAfee, 2009) but there is evidence that businesses, for example, banks, telecoms companies and other service providers severely under-report cybercrime committed against them. Jamieson *et al.* (2008) and Ehuan (2010) argue that the reason for this is that such organisations fear that publicly admitting victimisation could damage their reputation and generate bad publicity, or might even end in legal proceedings against them if they have lost personal data. Ferwerda *et al.* (2010) report that many companies view the public acknowledgement of security vulnerabilities as a corporate liability.

Lovet (2009) cites the 2008 Computer Crime and Security survey from the US-based Computer Security Institute which reports that when they were victims of cybercrime offences, only 27 percent of organisations (both from private and public sector) reported them to a law enforcement agency.

Lack of specific legislation on cybercrime

Blanco-Hache and Ryder (2011) citing relevant reports by the UK House of Lords argue that with no agreed cross-border classification of technology-related crime, the ability to distinguish or quantify the true scale and criminal nature of cybercrime remains extremely difficult (House of Lords, 2008; House of Lords Science and Technology Committee, 2007).

There is a template for legislation in the Convention on Cybercrime, but as of October 2011 only 29 countries have ratified the Convention (Council of Europe, 2011). The current status of Treaty shows that many Eastern European countries such as Bulgaria, Ukraine and Romania have signed and ratified the Convention, whereas until recently Sweden (23/11/2001), Ireland (28/02/2002) and Belgium (23/11/2001) had signed but had not ratified it. Internationally, the USA (25/05/2011) has both signed and ratified the Cybercrime Convention, while Canada, Japan and South Africa have signed but not ratified. The Russian Federation has refused to sign the Convention citing disagreement on terms for cross-border access to data processing networks.[10]

The technical difficulty of investigation and prosecution

Even when crimes are reported, investigation and prosecution remain difficult. Evidence is often ephemeral and transitory, and the global nature of cybercrime presents serious difficulties in pinpointing the location and identity of criminals (Ferwerda *et al.*, 2010).

It is often technically and legally difficult to gather evidence where the perpetrator is physically distant from the victim. Many local and state law enforcement agencies lack the technical sophistication of the most effective Internet criminals (Swire, 2009).

The harm caused by cybercrime is often intangible or indirect

Compared to a crime committed against a person or property, it can be difficult to assess the true monetary damage of cybercrimes such as information theft or security breaches. Given that law enforcement agencies possess limited resources this ambiguity surrounding the impact of cybercrime can mean that investigating and prosecuting such cases are not a priority for police forces.

Transnational factors

Victims and perpetrators are usually not in the same jurisdiction and national enforcement agencies might be less incentivised to prioritise investigation of harms that occur across borders. It might not be clear which court has jurisdiction over a particular cybercrime (Harbell, 2010).

What do available measurements and statistics say?

In this subsection we draw on information reported in the following data sources:

- The Internet Crime Complaint Centre (IC3):[11] This is a US-based organisation which receives Internet-related criminal complaints.

[10] For example, according to remarks made at the 17th ASEAN Regional Forum, 2010, "Russia being a member of the Council of Europe did not sign the said Convention because of article 32 "b" (Trans-border access to stored computer data), which makes possible for one Party to access or receive through a computer system in its territory, stored computer data located in other Party without notification of its official authorities. Article 32 "b" contradicts Russia's legislation and affects its sovereignty. The existing possibilities of misusing the Convention do not, in fact, facilitate international co-operation in such a sensitive field, but make it very problematic for Russia."

[11] A US organisation which is a partnership between the Federal Bureau of Investigation (FBI), the National White Collar Crime Centre (NW3C), and the Bureau of Justice Assistance (BJA)

- The European Source Book of Crime and Criminal Justice Statistics (2010). This report is published by the Research and Documentation Centre at the Dutch Ministry of Security and Justice and is based on gathering data collection from national correspondents across European Countries.

The figures presented in this subsection should be treated cautiously, given what has been said above about the limitations of statistics on cybercrime. Furthermore, as will become apparent, much of the cost estimates identified in our desk research stem from English-speaking countries – specifically the United States of America, United Kingdom, Canada and Australia.

Estimates from the IC3

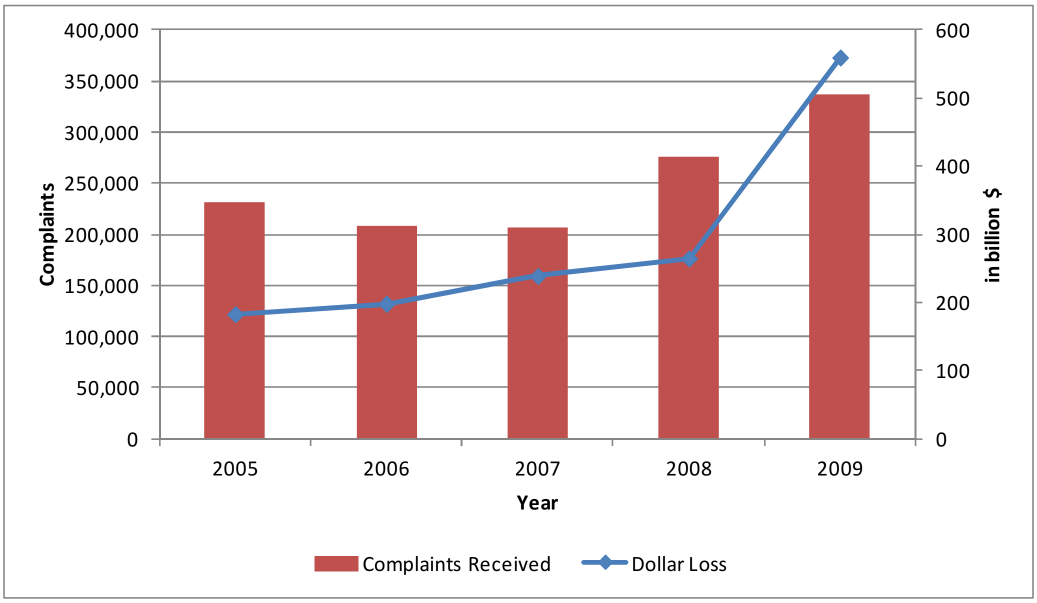
Figure 2.6 (below) shows the numbers of complaints received by the IC3 between 2005 and 2009.

In 2008, the IC3 processed over 275,000 complaints. Of those complaints, 26 percent were deemed valid and referred to law enforcement agencies (Ferwerda *et al.*, 2010). The top cybercrime complaint categories in 2010 were (IC3, 2011):

- Non-delivery (paying for merchandise online, but not receiving it)
- Auction fraud
- Debit/credit card fraud
- Confidence fraud (also referred to as advance-fee fraud)
- Computer fraud
- Check fraud[12],
- "Nigerian 419" schemes (letter fraud)
- Identity theft
- Financial institutions fraud.

[12] The inclusion of cheque fraud in the list of cybercrimes as defined by the IC3 is in and of itself insightful regarding the definitional complexity of cybercrime.

Figure 2.6 Online crime complaints and dollar loss in the United States



Source: IC3 (2010)

An increase in the number of complaints reported might not indicate an increase in the number of crimes, but could result from growing public awareness of the reporting centre. It is nonetheless interesting to note that the majority of crimes identified here related to fraud or scams. Contrast this list, for example, to the proposed framework from Alaakbi and it is possible to discern that most forms of "cybercrime" identified above detail the second type of offences where the computer is the tool. Nonetheless, we can see that it would appear that within these types of offences the dollar loss per complaint is increasing.

European Source Book of Crime and Criminal Justice Statistics (2010)

The European Source Book of Crime and Criminal Justice Statistics 2010 provides information on police-reported cybercrime offences, presented under the heading "Offences against computer data and systems". These offences are defined as follows:

> "offences against the confidentiality, integrity and availability of computer data and systems"

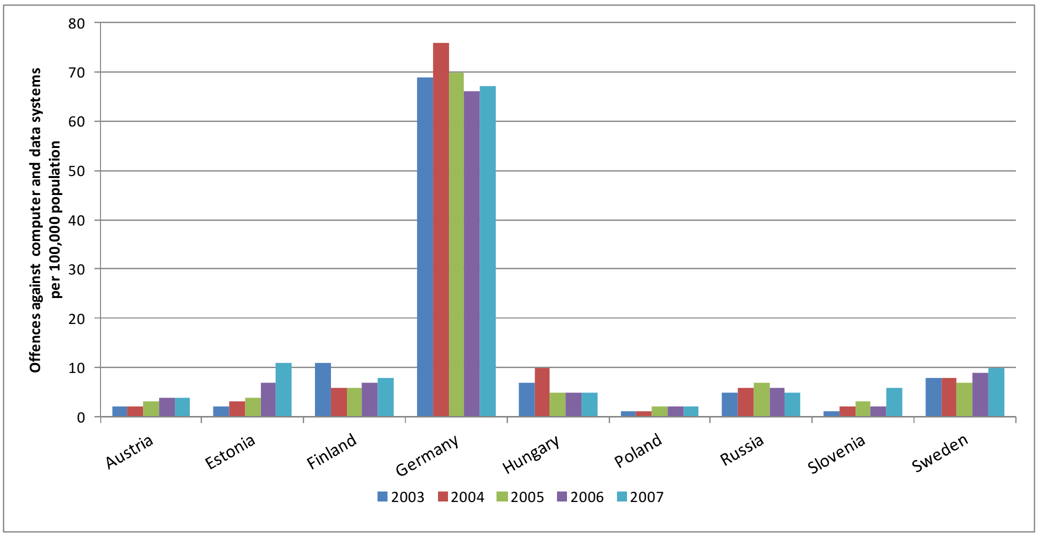
This is comprised of: unauthorised entry into electronic systems (computers) or unauthorised use or manipulation of electronic systems, data or software. Where possible, the figures exclude illegal downloading of data or programs, but include:

- Illegal access (i.e. intentional access to a computer system without right, e.g. "hacking").
- Illegal interception (i.e. interception without right, made by technical means, of non-public transmissions of computer data).
- Data interference (i.e. damaging, deletion, deterioration, alteration or suppression of computer data without right).

- System interference (i.e. serious hindering without right of the functioning of a computer system).
- Misuse of devices (i.e. production, sale, procurement for use, import, or distribution of a device or a computer password/access code).
- Computer fraud (i.e. deception of a computer instead of a human being).
- Attempts to carry out any of the above.

Figure 2.7 presents the number of offences in "computer and data systems" across countries during the period 2003–2004. Out of the 40 countries surveyed in the European Sourcebook, countries with missing data or zero offences for any year are not shown in Figure 2.7.

Figure 2.7 Offences against computer and data systems



Source: European Source Book (2010)

The average number of offences against "computer data and systems" across the countries above exhibits small variations and lies within the range of 6–8 per 100,000 population during the period 2003–2007. Excluding Germany as an outlier, within the same period, the median varies between one police-recorded offence per 100,000 (2003) and three per 100,000 (2005). There is a median equal to two police-recorded offences per 100,000 head of population in 2007. On the other hand, there are extremely large increases and decreases within country increase during the period 2003–2007. For example (not shown above), according to the European Sourcebook, Croatia has experienced an increase of more than 1,000 percent in police-recorded offences and Moldova has experienced a decrease of 88 percent police-recorded offences in the category of "computer data and systems" offences during 2003–2007, respectively.

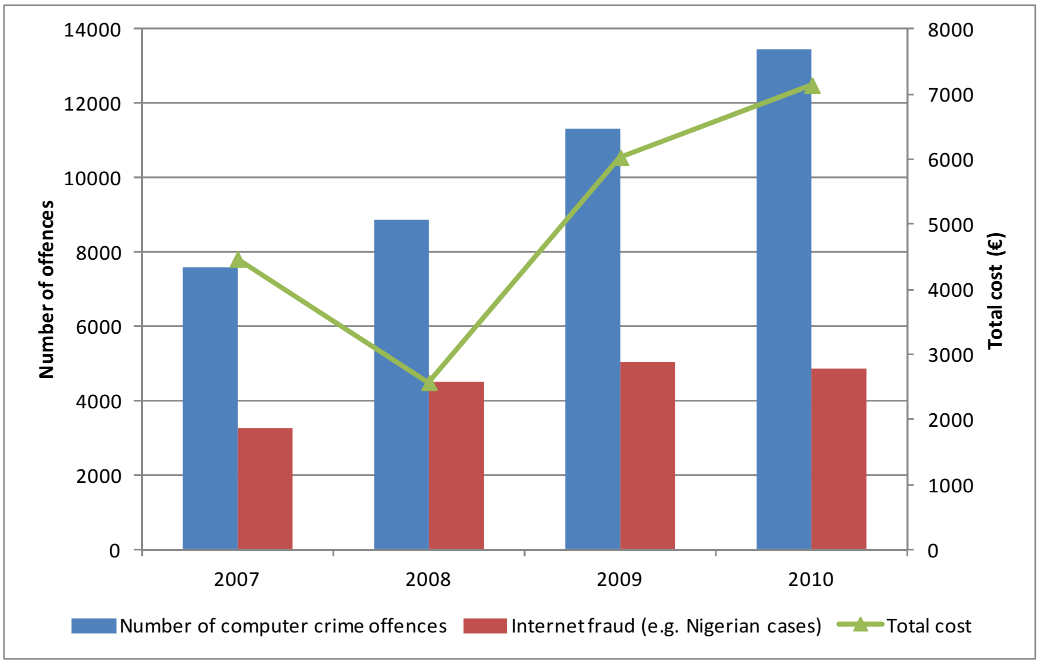
The report also includes figures on fraud. While all countries have provided data for this type of offence, quite a few could not adopt a standard definition, so it is likely to include all types of fraud including cyberfraud.

European Member States' data about cybercrime

We were able to identify recent data on cybercrime from some EU Member States. In some cases we were pointed to this data during interviews with Member State High-Tech Crime Units (or the equivalent). In other cases we identified data during our literature review. Of course, these are recorded cybercrime figures either from the cybercrime units' own management information systems or from official reports, and thus depend upon the particular reporting and recording mechanisms in each country. Further, we have no information about how the data have been processed and cleaned within each of the Member States. We can also make no comparative analysis between countries. With these caveats, the information we were able to collect is presented here.

- Data from the Austrian Federal Ministry of the Interior indicates that in 2001 there were 600 "Internet crimes" compared to 5,100 cases in 2011. What constituted Internet crimes was not defined in the report. Hacking was reported to have increased by 70 percent from 142 cases to 241 cases (it is assumed that this increase occurred over the same time period) (Bundeskriminalamt, 2011). This report also states that in 2010, there were 667 cases of credit card fraud reported whilst in 2011 there were 1,117 reported cases. Furthermore, this same source reported 790 frauds conducted through mobile 'phones in 2010 compared to 1,152 in 2011.
- Belgium provided information about the number of computer crime offences and Internet frauds in 2007, 2008 and 2009 and the cost of Internet fraud from their annual reports. This is set out in Figure 2.8.
- Germany provided information about some recorded cybercrimes in 2009 and 2010 from official annual reports. This is set out in Figure 2.9 and Figure 2.10.
- Italy provided information about reports to their online police station (Figure 2.11), the number of websites monitored by the Centro nazionale per il contrasto alla pedo-pornografia su Internet (National centre combating online child pornography), about arrests, seizures and reports processed by CNCPO (Figure 2.12), and data collected by the Centro Nazionale Anticrimine Informatico per la Prottezione delle Infrastrutture Critiche (National Centre for cybercrime and critical information infrastructure protection, CNIPIC) (Figure 2.13).
- Slovenia provided information for 2007, 2008, 2009 and 2010 about the numbers of attacks on information systems; intrusion into business information systems; and "the production and acquisition of weapons and instruments intended for the offence" (taken to mean malware) (Figure 2.14).

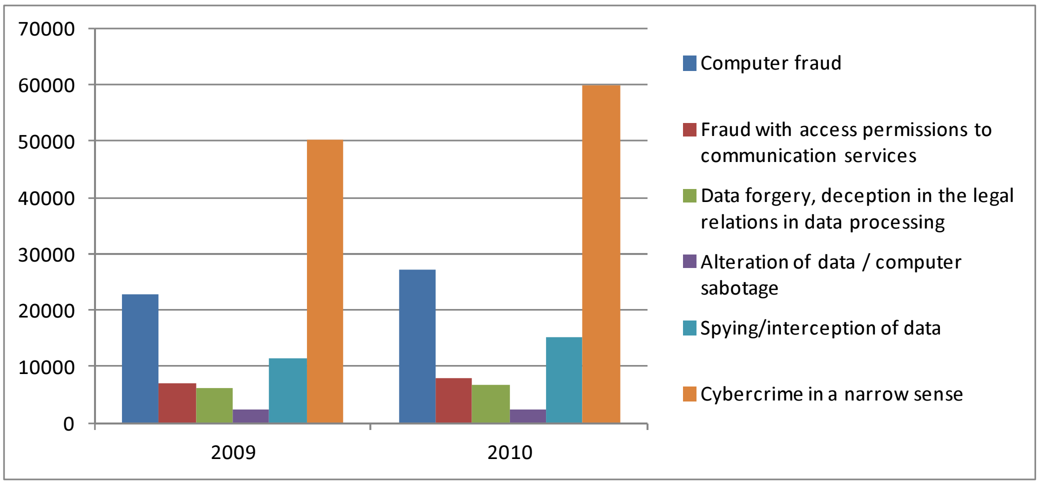
Figure 2.8 Belgium: recorded computer crime offences, Internet fraud and total cost



Source: Report of the Belgian Economic and Financial Crimes Division (DJF)

In Figure 2.8 above, we can observe that in Belgium the number of recorded offences is growing for computer crimes but largely flat for Internet frauds. We can also observe a trend of increasing total cost – although data were not provided to show whether this cost was at 2010 or 2007 Euro rates (i.e. accounting for inflation) nonetheless we can readily observe an upward trend.

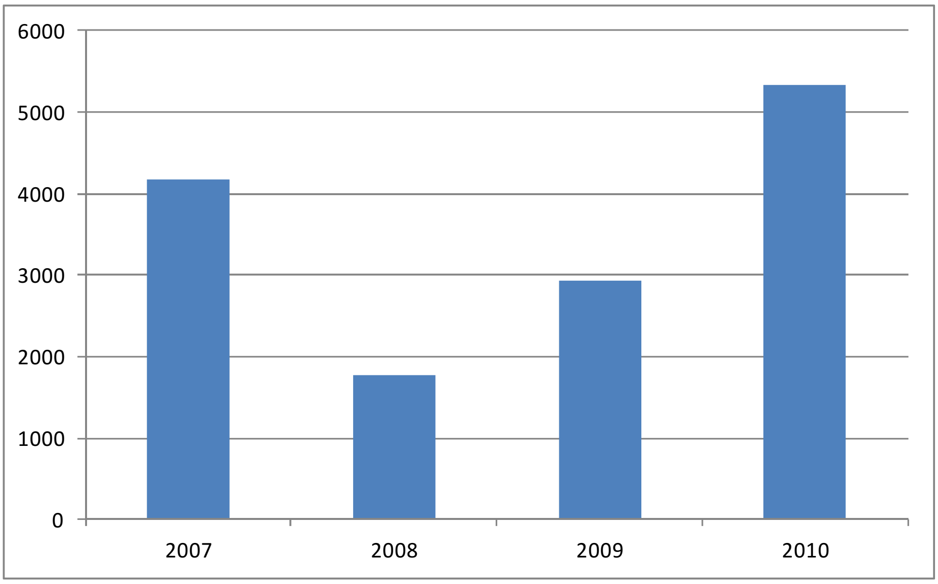
Figure 2.9 Germany: recorded cybercrimes



Source: German Annual Federal Criminal Police Office Situation Report on Cybercrime 2009 and 2010

In recorded cybercrimes in Germany we can see that between 2009 and 2010 there was an increase in computer fraud and cybercrime in a narrow sense (which we take to mean attacks against information systems). This data is instructive in the way in which, as well as showing a general trend of increase, it also splits the types of cybercrime into different categories relating to whether the computer or information system is the tool or the target of the attack.

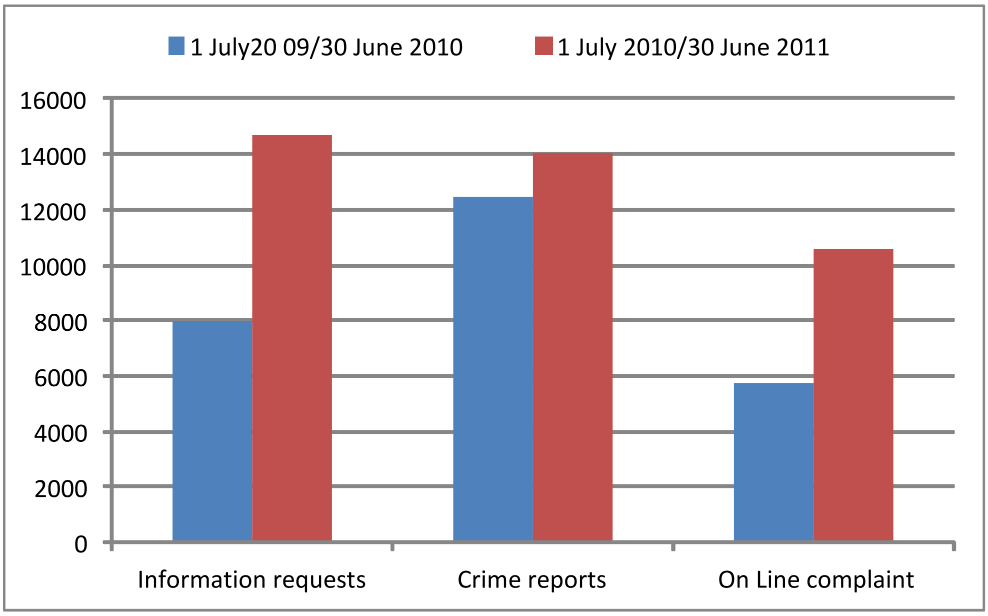
Figure 2.10 Germany: recorded cases of phishing in online banking



Source: German Annual Federal Criminal Police Office Situation Report on Cybercrime 2009 and 2010

According to the official German Criminal Police Office statistics we can observe the trend of an increase between 2008 and 2010. There is no explanation as to what accounts for the dip between 2007 and 2008. Perhaps this was the result of a change in how records were collected or some other aspect of data collection.

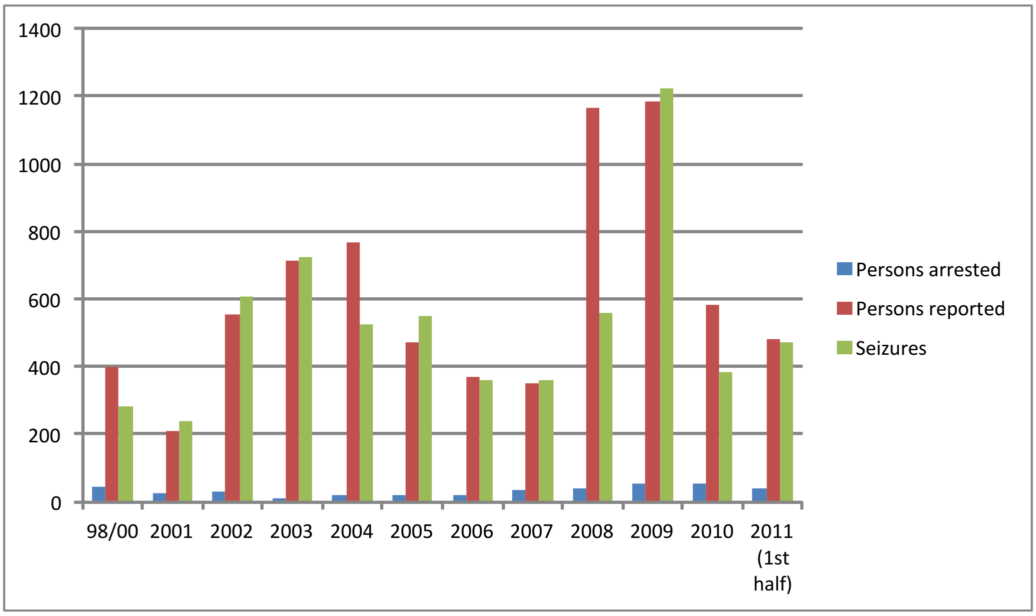
Figure 2.11 Italy: online police station – information requests, crime reports and online complaints



Source: data provided by Postal and Communications Police

Turning to Italy, Figure 2.11 above shows an increase across the board of information requests, crime reports and online complaints (with information requests and online complaints increasing more rapidly than crime reports) between 2010 and 2011. Although it is possible to observe an increase across both time periods it is interesting to note that the pattern between information requests and crime reports changed in the period 1 July 2010–30 June 2011, with the number of information requests and crime reports being more or less equal, compared to the same period for the previous year. One possible explanation might be that awareness of how to make information requests changed between the reporting periods (but still had no effect on crime reports).

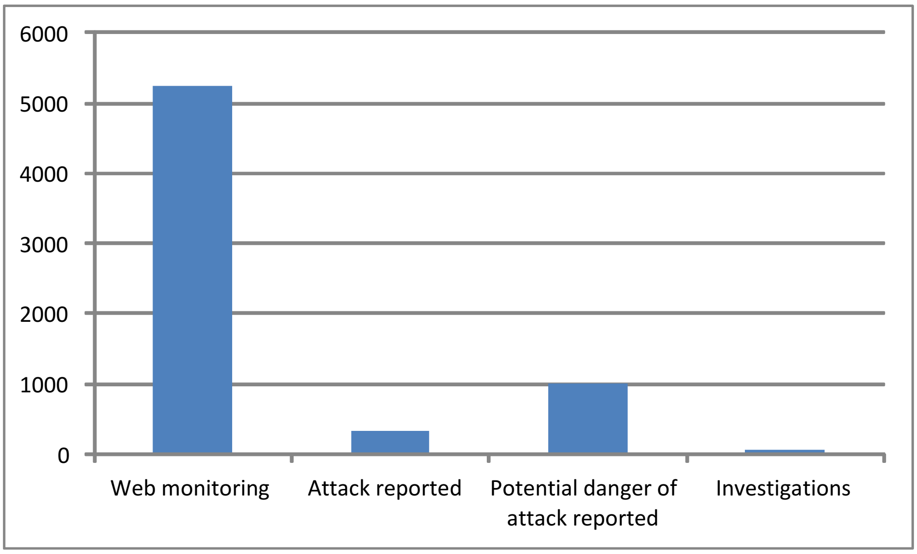
Figure 2.12 Italy: arrests by, reports to and seizures by CNCPO



Source: data provided by Postal and Communications Police

Figure 2.12, again from Italy, illustrates the low ratio between seizures of material (assumed to be hard disk drives, PCs, etc.) and arrested persons. The large variations in the data are interesting particularly both for 2008 and 2009 (both within figures such as seizures and arrests and also between different categories). The discrepancy might be the result of changes in recording this data or perhaps an awareness campaign run by the Italian police. Either way, a cyclical trend is clear; but as with many other forms of statistics in the law enforcement realm, it is difficult to see whether this is a pattern in the actual phenomena or just reflective of the resources of law enforcement.

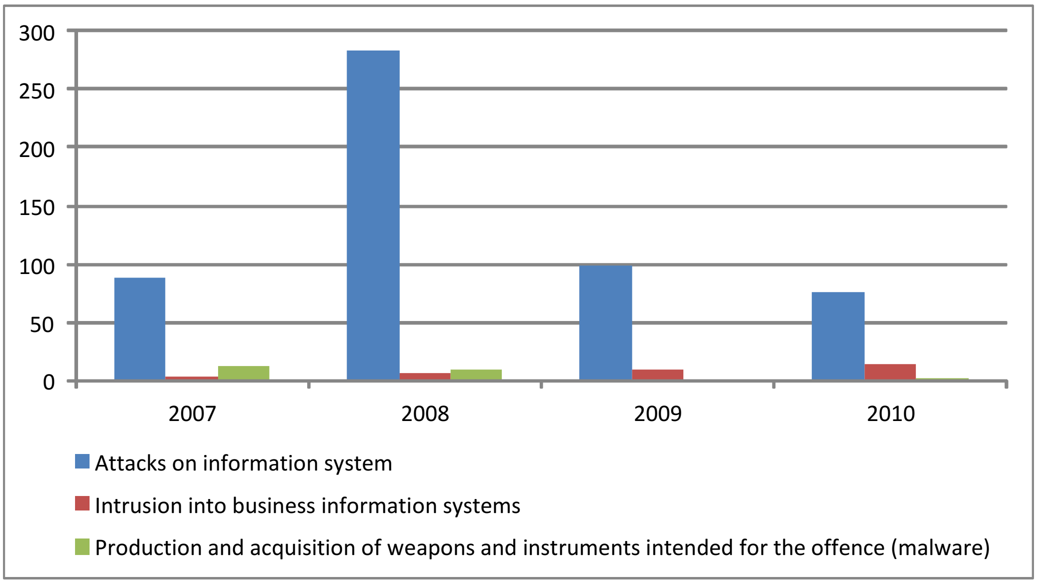
Figure 2.13 Italy: activities of the CNAIPIC 1 June 2010–30 June 2011



Source: data provided by Postal and Communications Police

Figure 2.13 above also illustrates the low ratio of actual investigations to other forms of input that a cybercrime unit might see, including monitoring the Internet for criminal activities and reports of attacks.

Figure 2.14 Slovenia: recorded attacks/intrusions/production and acquisition of weapons intended for the offence (malware)



Source: data provided by Slovenian national unit

Finally, Figure 2.14 above illustrates for simple comparison purposes how the number of attacks outweighs both the recorded numbers of intrusions and arrests for malicious code. This is suggestive of the way in which technology plays a multiplying role with respect to actual attacks.

2.6 What are the available estimates as to the cost of cybercrime?

Estimates of the total cost to society of cybercrime vary, and given the lack information about the extent of the harm caused by cybercrime, such estimates must be treated with much caution. In this section we set out estimates generated by different organisations, but it is beyond the scope of this review to examine the methodologies and approaches used to generate these estimates.

It is also instructive to illustrate how these inform (or not) the somewhat paradoxical logic of the policy debate concerning cybercrime. For example, in 2007 the House of Lords published a report which said:

> "While the incidence and cost of e-crime are known to be huge, no accurate data exist."[13]

This exposes an underlying challenge with the phenomena of cybercrime. Current established wisdom is that this is a big problem, but policy-makers, law enforcement and others complain about a lack of data and reliable evidence as to the extent.

Furthermore, in some instances it is possible to observe somewhat differing approaches to the definition of cybercrime between what was presented above and what might be included under the phenomena in order to inflate costs. The 2011 Norton Cybercrime Report is a case in point (Norton, 2011). The majority of definitions used to frame the questions in that study detail activities relating to what is understood earlier as "misuse of communications" – for example, bullying online or via a mobile 'phone, "cyberbaiting" or receiving age-inappropriate content via communications devices.

The Norton survey did include asking respondents whether they had received computer viruses or malware, responded to a phishing message, hacking of a social networking profile, responded to an online scam, or were a victim of identity theft. In general, the definitions and contextual understanding of that study (which has been widely quoted) appear to revolve around those types of cybercrime where the computer is the tool used to perpetrate "traditional" forms of crime (fraud, bullying, harassment, etc.) rather than necessarily the target.

[13] House of Lords Science and Technology Committee Report (2007)

Box 2.2 Inconsistencies in the presentation of evidence found in the academic literature

Robust, reliable, longitudinal evidence on attacks, threats and impacts (economic and non-economic) of cybercrime is rather limited. It concentrates on anti-virus corporations (e.g. McAfee, Symantec), the US Government (IS3), the EU (e.g. Sourcebook on Cybercrime) and international organisations such as the OECD.

During our endeavour to identify this evidence, we have also collected evidence from journal publications from academia. We have come across several cases in which evidence provided by the above organisations is accompanied by the wrong citation – i.e., researchers tend to cite the report or publication in which the above evidence was mentioned, for the sake of argument, and not the original source of the data.

Below we provide two examples:

Example 1: "The total amount of money involved with credit card fraud is estimated at €375.3 million (or US $400 million) annually"
We first identified the above statement in Deflem and Shutt (2006) who report this figure as part of their discussion on cybercrime. Their paper cites Aldesco (2002) when providing the above evidence. Further, Aldesco (2002) refers to a press release from the Council of Europe which is no longer available online. The actual information comes from Mastercard and was reported in 1998 at a US congressional briefing (Congressional Record, 1998).
The above demonstrates that is a difficult to assume that there is enough of evidence on credit card fraud, and most importantly what portion could be attributed to cybercrime given the date of the report (since it is possible that between 1998 and 2006 the proportions of credit card transactions over the Internet evolved).

Example 2: "The cost of a botnet is $0.04 (2009) and $0.03 (2010)"
As part of our search in the academic and grey literature, we found that Sommer and Brown's OECD report (2011) attributes the above evidence to a House of Lords, EU Committee report (2010), which correctly cites Symantec's report (Symantec, 2010).

Overall estimates including different types of cybercrime

In 2011 Norton (a global cybersecurity firm) released its Annual Report into the global costs of cybercrime. This exercise over 24 countries interviewed nearly 20,000 people. The Norton Cybercrime Report estimated that the "total global cost of cybercrime" was US $114 billion. If the reported estimate of their lost time was included then this rises by an additional US $274 billion to an overall total of US $388 billion. Although this report uses definitions that fit (to a certain degree) with those presented previously, it is not known how the estimate of the costs of lost time was determined. The report goes on to compare the cost of cybercrime (unfavourably) with the global costs of marijuana, cocaine and heroin markets by way of providing some context (Norton, 2011 #111).

Blanco-Hache and Ryder (2011) point out that online crime costs the average small business in the UK €932 (£800) a year (2009 prices) (Federation of Small Businesses, 2009). The Association of Chief Police Officers of England (ACPO) said online crime cost €76 billion (£52 billion) worldwide in 2007 (Association of Chief Police Officers of England, 2009).

In a widely quoted study of May 2011 by Detica for the UK Home Office, cybercrime was reportedly costing the UK €30 billion (£27 billion) a year – €21 billion of which was attributed to UK businesses. However, much of this was attributed to "less understood cybercrimes including:

- Identity theft and online scams affecting UK citizens
- IP theft, industrial espionage and extortion targeted at UK business
- Fiscal fraud committed against the government" (Detica, 2011).

The cost of identity theft in the USA, Canada, UK and Australia

Jamieson *et al.* (2008) summarise data from a number studies about the cost of identity theft and fraud in the USA, Canada, UK and Australia.

- According to the US Federal Trade Commission, in 2005 the costs of "identity theft" were €4 billion (US $5 billion) for American consumers and €38.5 billion (US $48 billion) for businesses, respectively (Ilett, 2006).
- In the same year, the estimated cost of identity fraud[14] in the UK was €2.5 billion (£1.7 billion), an increase from €2 billion (£1.3 billion) in 2002. However, a revised estimate was produced at €1.767 billion (£1.209 billion), or €36.5 (£25) for every adult in Britain, in 2007. The UK Government made clear that the 2007 estimate was a one-off and that future cost exercises would be based on a new, more robust methodology that was being devised by the Identity Fraud Steering Committee (IFSC). The updated estimate was produced through liaison and discussions with private- and public-sector organisations and represented a best estimate of the scale of the problem at that time, which captures available information. The new methodology devised by the IFSC does not examine the financial loss to an organisation, or costs incurred to set systems in place to identify, prevent, deter and prosecute cases of identity fraud (UK Home Office, 2006).
- In the period 2001–2002, the cost of identity fraud to individuals in Australia was €635.1 million (AUS $1.1 billion) a year (Cuganesan and Lacey, 2003).
- During the same period, the Canadian Council of Better Business Bureaus estimated that consumers, banks, credit card firms, stores and other businesses lost €1.68 billion (CAN $2.5 billion) to the perpetrators of identity theft in 2002 (Brown and Kourakos, 2003; Canadian Bankers Association, 2003).

Jamieson *et al.* (2008) conducted a series of interviews involving 27 experts in fraud, finance, accounting, legal, and ex-law enforcement in the United States. The authors found that losses from indentify theft amounted to €45.5 billion (US $56.6 billion) in 2005, falling to €40.6 billion (US $51 billion) in 2006 and €32.8 billion (US $45 billion) in 2007.

Credit card fraud

Lemiex (2011) reports a US Federal Bureau of Investigation (FBI) study in which a typical loss in 2010 is estimated at €168 (US $223) for credit card fraud per complaint.

Shutt and Delfem (2006) report that the total amount of money involved with credit card fraud is estimated at €375.3 million (US $400 million) annually (1999 prices) in the USA alone. This amount comes from consumer reports by Mastercard and its member banks

[14] It is assumed that this is a comparable term to that used in the United States of "identity theft"

(Congressional Record, 1998) but it is not known whether this excludes or includes online frauds.

Malware, phishing and spam

Reliable empirical information on the operational and financial aspects of malware (and spam) is difficult to collect. Available estimates of attack trends and damages are provided by security-service providers. These are often the only available figures and need to be considered in context: security-service providers may have an incentive to overestimate security problems (ITU, 2008). Other information is considered proprietary or only reported if the damage exceeds a certain threshold. Finally, there are serious gaps and inconsistencies in the available information on the financial aspects of malware and spam. This sketchy information base also complicates finding meaningful and effective responses. The wide range of values documented is presented in the following table (ITU, 2008).

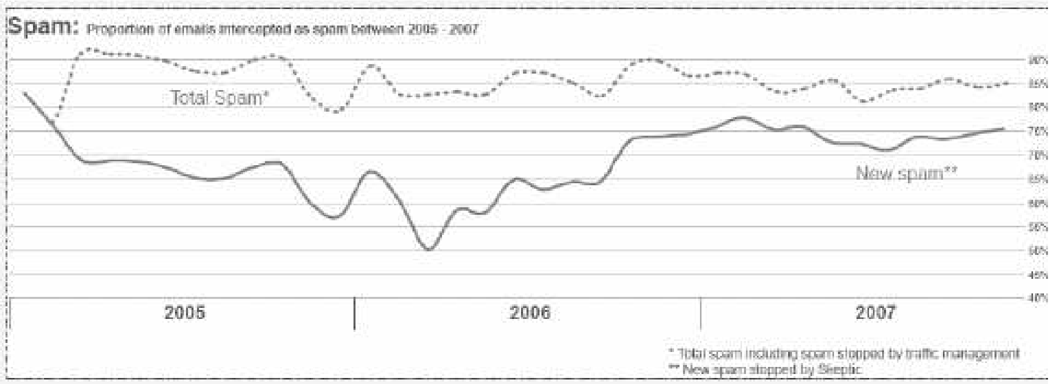
Table 2.1 Estimated costs of malware, spam and click fraud

Type of malevolent software	Target	Costs/damages
Malware	Businesses	Globally: €10.6 billion (US $13.3 billion) in 2006 – Source: Computer Economics US: €54 billion (US $67.2 billion) in direct and indirect effects on US businesses alone in 2005 – Source: FBI
Malware and spam	Consumers	US: €5.2 billion (US $7.1 billion) in 2007 – Source: State of the Net survey projections
Spam	Businesses	Globally: €72.97 billion (US $100 billion) in 2007 – Source: Ferris Research US: €25.5 billion (US $35 billion) – €51.8 billion (US $71 billion) in 2007 – Source: Ferris Research and Nucleus Research Inc.
Click fraud	Businesses	US: €730 million (US $1 billion) in 2007 Source: ITU, (2008)

Hartel *et al.* (2010) cite the Gartner Group report in which it is estimated that in 2008 each of more than five million US consumers lost on average €238 (US $350) due to phishing scams, and that the number of cases is rising, while the average loss is falling.

As reported by MessageLabs Intelligence (2007) and shown Figure 2.15 below, 85–95 percent of e-mails globally have been considered spam during the period 2005–2007. According to these data, the overall proportion of spam intercepted in 2007 was around 84.6 percent of the total number of e-mails, compared to 86.2 percent in 2006. Of this volume, 73.9 percent was from new and previously unknown sources as compared to 63.4 percent for 2006.

Figure 2.15 Spam rates 2005–2007



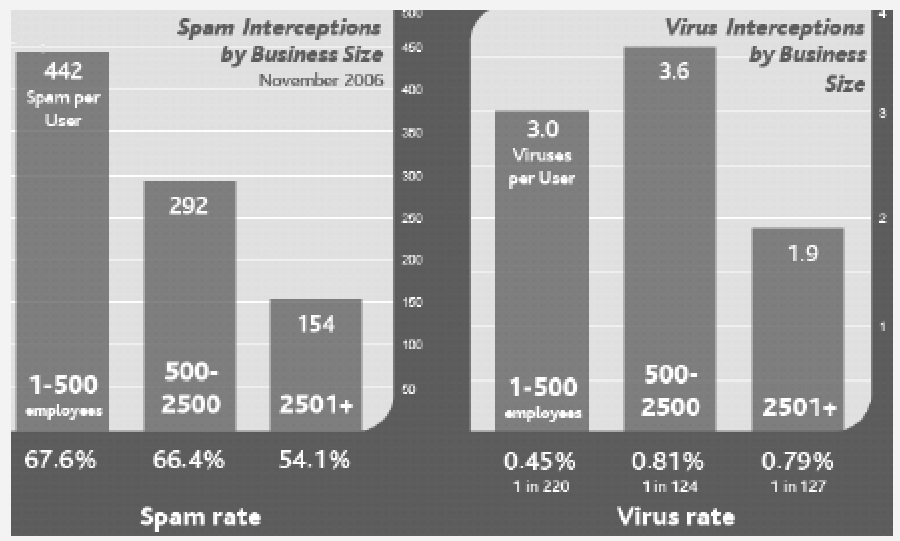
Source: MessageLabs Intelligence (2007). Adapted from ITU (2008)

Viruses/malicious code

Shutt and Delfem (2006) report that the so-called Love-Bug worm that spread via e-mails to millions of computers in the spring of 2000 led to an estimated €7.25 billion (US $6.7 billion) in damages and may have cost as much as €10.83 billion (US $10 billion) in lost productivity worldwide.

In November 2006, MessageLabs studied the demographics of the businesses targeted with spam. Their survey revealed that small- to medium-sized businesses (1–500 employees) are targeted with three times more spam per user per month than the larger enterprise clients (2,500+), and almost twice as much as medium-sized (501–2,500) corporate clients) (see Figure 2.16, below).

Figure 2.16 Spam and virus interception by business size

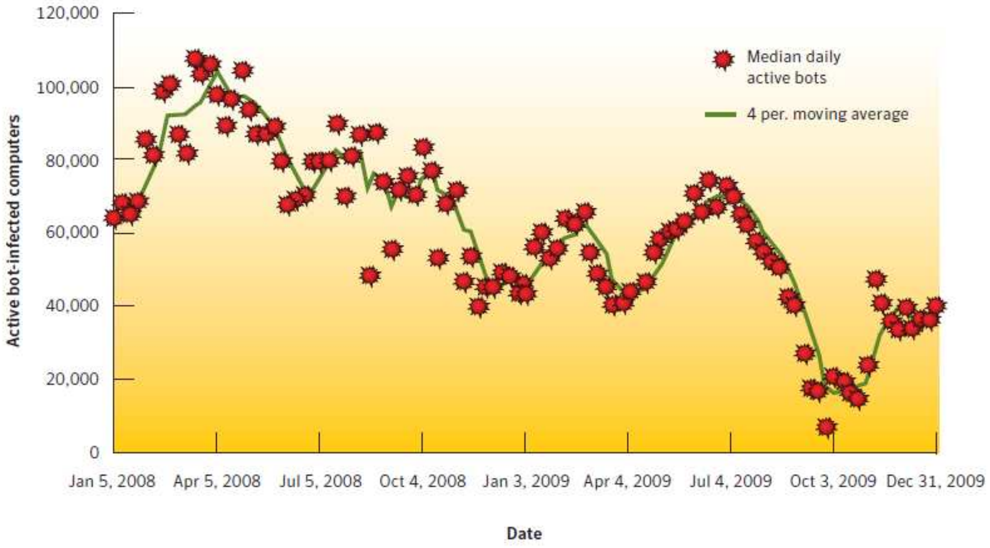


Source: MessageLabs Intelligence (2007). Adapted from ITU (2008)

Botnets

In 2009, Symantec observed an average of 46,541 active bot-infected computers per day (Figure 2.17), which represented a 38 percent increase from 2008. Also, Symantec observed 6,798,338 distinct bot-infected computers during 2009 – a 28 percent decrease from 2008. This decrease is primarily considered the result of bots sending larger volumes of spam instead of propagating, or performing non-typical activity that is not being monitored. In the underground economy, Symantec observed advertisements for as little as €0.02 (US $0.03) per bot. (Guinchard, 2011; Symantec, 2010).

Figure 2.17 Active bot-infected computers, by day



Source: Symantec (2010)

Patents and trademarks

Profits lost by firms from stolen patents and trademarks was estimated by the Council of Europe in its 2002 report at €264.4 billion (US $250 billion) – nearly 5 percent of world trade (Aldesco, 2002). Whilst such costs are not associated with attacks against the confidentiality, availability or integrity of computers or information systems, they are facilitated by technology (and in some cases might be made possible through technology vulnerability) but in certain circumstances the costs may be reported as "cybercrime" – e.g. the Detica May 2011 report for the UK Home Office (Detica, 2011).

Black market for personal data

PandaLabs[15] – an anti-malware laboratory – investigated the black market for cybercrime. They discovered a vast network selling stolen bank details along with other types of products in forums and more than 50 dedicated online stores. Table 2.2 below presents a summary of the products in the available cybercrime black market and their prices.

[15] As of 15 February 2012: http://www.pandasecurity.com

Table 2.2 Prices of cybercrime products

Products	Price*
Credit card details	From €1.5 (US $2) to €68 (US $90)
Physical credit cards	From €136 (US $180) + cost of details
Card cloners	From €151 (US $200) to €754 (US $1,000)
Fake ATMs	From €2,640 (US $3,500)
Bank credentials	From €60 (US $80) to €528 (US $700) with guaranteed balance
Money laundering	From 10 to 40 percent of the total From €7.5 (US $10) for simple accounts without guaranteed balance
Online stores and pay platforms	From €60 ($80) to €1,312 (US $1,500) with guaranteed balance
Design and publishing of fake online stores	According to the project (not specified)
Purchase and forwarding of products	From €23 (US $30) to €226.3 (US $300) depending on the project
Spam rental	From €11 (US $15)
Simple Mail Transfer Protocol (SMTP) rental	From €15 (US $20) or €30 (US $40) for three months
Virtual Private Network (VPN) rental	€15 (US $20) for three months

* 2010 prices rounded to the nearest digit

Source: : PR Newswire (2011)

We discuss below in the concluding section overall trends with respect to costs, complexity and what conclusions may or may not be drawn from these data.

2.7 What do we know about the nature and complexity of cybercriminals?

The United States Secret Service (USSS) and the Dutch National High-Tech Crime Unit (NHTCU) undertook analysis of 800 data compromise incidents (Baker *et al.*, 2011). The data for their report comes from the combined caseload of telecommunications company Verizon and the United States Secret Service (USSS). However, the authors do stress that it is not possible to measure sample bias or to identify what percentage of data breaches are represented as it is not possible to know the total number of data breaches across all organisations in the USA. These incidences were confirmed or investigated in different countries across the globe including Australia, Belgium, Canada, China, France, the UK, USA and others.

Ninety-two percent of the data breaches they examined stemmed from “external agents” including organised criminal groups (58 percent of cases examined), unaffiliated person(s) (40 percent), former employees (2 percent), competitors (1 percent), unknown (14 percent), and other (<1 percent). Fifty percent utilised some form of hacking, 49 percent incorporated malware and 29 percent involved physical attacks. Overall, Baker *et al.* (2011) argue that 92 percent of the attacks analysed were “not highly difficult”.

The same report outlines that in 2010, the top three industries in the sample of incidents analysed were hospitality (40 percent), retail (25 percent) and financial services (22 percent). This report finds an increase of 22 percent between 2009 and 2010 in small external attacks (Baker *et al.*, 2011).

The 2011 European Electronic Crime Task Force (EECTF) European Cybercrime Survey (2011) focuses on Europe and gathers information from law enforcement authorities, businesses, security-solution providers, intelligence agencies and experts. Participants provided their contribution via three separate channels: questionnaires, reports and analyses, and direct interviews. The report argues that the number of online frauds/cyberfraud is rising worldwide, but that average profit per attack is dropping, at least for certain types of fraud. The authors argue that this phenomenon might be explained by the increasing awareness of users and the proliferation of effective countermeasures against the most common attacks, which would indicate that the economic damage of cyberfraud is not proportionate to the intensity of the attacks. Finally, the report highlights that this has resulted in an increase in the number of attempts to compromise systems: criminal organisations must raise the intensity of attacks to maintain their profits (EECTF, 2011).

In addition, the authors were able to identify geographical clusters from where many cybercrimes reported in the EECTF report originated. These clusters include growing economies, such as Brazil and China, and others such as Russia (EECTF, 2011). However, it is important to stress that undertaking comparative analysis of the number of crimes committed from a particular country is highly problematic, given the paucity of reliable statistics.

The report suggests that cybercrime is characterised by two aspects: crimes can take numerous different forms in terms of expertise and attacks, and there exists a number of well-structured schemes and mechanisms that are typical features of organisations and markets focused on profit.

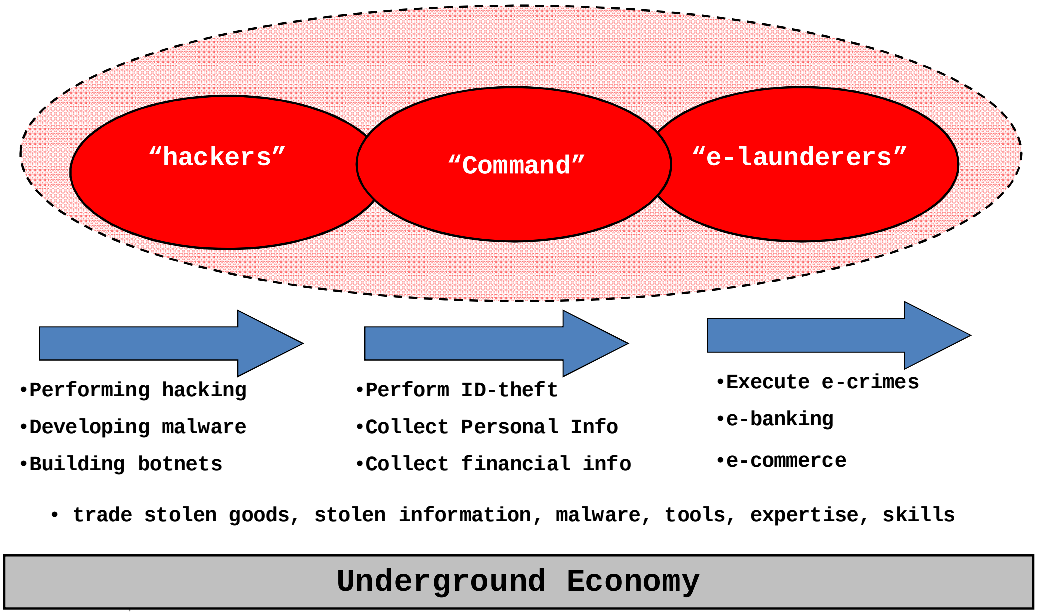
The USSS has focused enforcement efforts on “bulletproof hosters”. These companies offer web-hosting services that allow their customers considerable leniency in the types of materials they may upload and distribute. The authors argue that seizures in excess of 200 Terabytes (TB) of data belonging to bulletproof hosters have made the proliferation of malware more challenging for cybercriminals and provided a substantial number of investigative leads (Baker *et al.*, 2011). However, the report provides no evidence about the impact of data-seizure on cybercriminal activity.

Blanco-Hache and Ryder (2011) quote findings from the Garlik UK Cybercrime report (2009) where it is found that there was a 207 percent increase in bank-account takeovers between 2008 and 2009. The authors of the report argue that this finding indicates that criminals have shifted their efforts from opening new accounts with stolen identities to accessing existing accounts. The report also highlights that in the same period losses from online banking fraud increased by 132 percent, with total losses reaching €65.9 million (£52.5 million). This sharp rise can be mostly attributed to phishing websites specifically targeting banks and building societies in the UK.

The authors argue that the increase can be attributed, in part, to there being 43,991 phishing websites targeting UK banks and building societies in 2008, up 171 percent from 25,797 in 2007. The Garlik report finally stresses that estimating and quantifying cybercrime is an inherently imprecise activity comprising academic and grey literature (e.g. newspapers and conference proceedings), official publications and official and unofficial statistics.

A public abridged version of the Threat Assessment on Internet-facilitated Organised Crime (iOCTA) prepared by Europol touches upon the cybercriminal business model. The structure of the cybercrime business model differs significantly from the traditional theoretical understanding of organised crime. This is also true of other types of transnational crime, such as illegal people-trafficking, which do not adhere to hierarchical structures. Firstly, the business model of cybercrime is not hierarchical. There is no obvious leadership and labour is divided according to individuals' technical knowledge and specialisation in a similar way to the legitimate "service-led economy". Secondly, the demographic profile of cybercriminality also differs from traditional organised crime – namely young, highly skilled individuals who are often recruited from universities (Europol, 2011). This market-based model is represented below in Figure 2.18 from Europol's abridged iOCTA.

Figure 2.18 Cybercrime business model

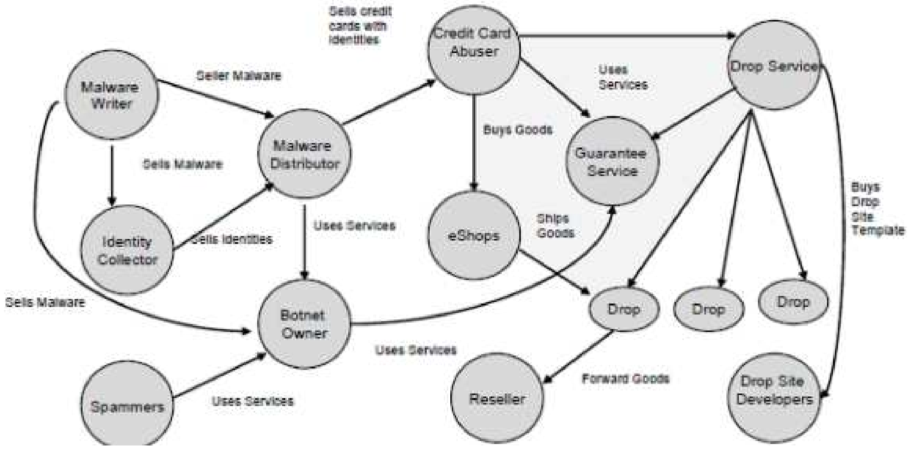


Source: Europol (2011f)

Also, direct contact is not necessary as most participants are able to interact using technological mediated communication tools (e.g. via instant messenger tools, online discussion forums or bulletin boards, etc.). Online forums facilitate recruitment and collaboration services. They also represent a degree of organisation at the administrative level. The actual organisation of cybercrime lies in its automation (Brenner, 2002). For example, using a botnet, cybercriminals can make use of thousands of compromised computers at a time to automate attacks on individuals and private businesses, send spam, host phishing websites, mount DDoS attacks, etc.

Monetisation of data is also essential to the cybercriminal enterprise. "Mules" are recruited via employment search and social networking websites to "cash in" stolen personal and financial information. As the individuals tasked with turning data to hard cash, mules are the visible face of cybercrime but are only conducting specific tasks as opposed to those commissioning their services.

Figure 2.19 Division of labour in the malware underground economy



Source: Adapted from MessageLabs Intelligence (2007)

As can be seen from the above graphic it would appear to be the case that the online criminal underground is even a stage beyond being networked. Wall (2008) argued that technological advancement has multiplied opportunities for criminal activity tilting the cost/benefit balance in their favour. If a cybercriminal can choose between performing a single high-risk bank robbery with the potential to net €5 million or five million "low-level" cybercrimes which allow him to defraud €1 each time then the choice is obvious. Cyberspace and the Internet infrastructure contribute to making cybercrime a "post-organised crime" phenomenon – a service-led model where there is no hierarchy, just crime service-providers unified by the infrastructure of cyberspace (Caballero et al, 2011).

2.8 Conclusions

In this chapter we have outlined the different types of misuse commonly understood to constitute cybercrime, reviewed current academic, legislative and practical approaches to defining and categorising these activities. We have also summarised some data concerning the quantity of different types of cybercrime and some of its costs and implications. This chapter has described why data on the numbers and nature of cybercrime provide a very limited evidence base for policy-makers and practitioners working in this field. It has made reference to a number of studies and data sources on the extent and costs of cybercrime, which require care and caution to interpret. Given these caveats, what conclusions, if any, might be drawn from these data? In this section we identify five broad trends which are indicated by the various information and data sources reviewed in this chapter – including criminal justice data, information from industry reports, and the data provided to the research team by Member States during interviews.

The data can indicate trends, but not the drivers

Both industry and criminal justice statistics show an increase in cybercrimes. Whilst 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 increase. 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 the reasons set out in Section 2.5, 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.

Cybercrime commonly has a financial motivation

Aside from revealing trends it is possible to identify some other pertinent factors from the available data. One of these is that, with the exception of Internet-facilitated child exploitation, many (but not all) of the types of crimes captured in the data sources outlined above are economic in nature rather than crimes against the person. There are sporadic reported cases of online bullying (e.g. attacks aimed at causing psychological harm to victims) through for example MMORPGs or social networking sites and some high-profile incidents of "hacktivism" (e.g. web defacements or attacks breaching SCADA networks) but the "volume" of cybercrime appears to comprise economically-motivated activities. If this is the case, there could be important knock-on effects beyond the losses suffered by individuals or companies. For example, the possibility that consumers may lose trust in e-commerce. At present there is little empirical research investigating the impact of the incidence of cybercrime on the take-up, level or extent of e-commerce.

Some indication that online criminal underground is increasingly complex

The appearances of offences and *modus operandi* such as botnet-herding in the data sources described above supports the argument made in the literature that the online criminal underground is increasingly complex and has characteristics in common with the legitimate "service-led economy". Unlike previous classifications of "organised crime" which turn on applying a definition of hierarchy, the understanding of the cybercrime underworld now most popular amongst those writing in the field is that there is a flourishing market of specialised service-providers, ranging from money mules who can bring the illegitimate gains into the licit economy, to coders who develop malicious code, to spammers and botnet-herders who can provide the platforms through which various types of misuse can be perpetrated.

Technology as a facilitator of cybercrime

The data sources above show an increase in the number of botnets over time (although they disagree on the actual numbers). This provides some supporting evidence for a third trend – that of the role of technology as a facilitator of different types of cybercrime, which might have financial, ideological or political motivation. This can be seen in particular regard to “botnets”. Botnets, as has been pointed out by the OECD (2008), can be understood as a kind of platform through which various types of misuse can be carried out – including attacks against the confidentiality, availability and integrity of computer systems but also preparatory acts and those which the Council of Europe loosely frames as crimes facilitated by technology. However, botnets may also be used as a platform to launch ideologically or even politically motivated attacks such as those conducted by supporters of Wikileaks against Amazon and Paypal in 2011.

It may be argued that the presence or absence of cybersecurity has a different impact depending on whether the crimes relate to attacks aimed at ICT or whether the crimes in question are instead facilitated by ICT. The implication would be that for those crimes where ICT is a facilitator or merely a characteristic of the investigation, efforts to address cybersecurity might have different impacts. This is because the latter, broader group of crimes, does not necessarily exploit security vulnerabilities or problems.

Cybercrime is evolving its technological sophistication

A final trend which finds some support in the available data is that technological sophistication has evolved. Where once e-mail-borne viruses and malicious code were the preferred attack vectors (which exploited vulnerabilities in desktop e-mail software) recent industry reports describe many pieces of malicious code that are highly sophisticated, blending a number of different technological aspects such as hiding their presence (e.g. deleting logs which might alert users to the presence of unauthorised software), polymorphism (changing the attack vector), encryption (to make it difficult for defenders to inspect the traffic that the programs may send out) and so on.

Conclusion

In summary, we can see that the aspects related to the phenomenon of cybercrime defy simplistic understanding; evolve rapidly in line with how society uses cyberspace; require technical knowledge to understand and the mapping of long term trends and patterns is fraught with complexity. In order to have any chance of success, a future ECC will need to conduct its activities in the context of these characteristics.

CHAPTER 3 The relationship between cyber(in)security and cybercrime

In this chapter we consider some broader issues which may affect the phenomena of cybercrime. In particular, we consider briefly the important relationship between cybersecurity and cybercrime. Because cybersecurity is a broad topic covering a range of ethical dimensions and socially important issues (relating to, for example, economic growth, innovation, Internet governance, protection of fundamental rights such as privacy and freedom of expression), we focus on only those aspects of cybersecurity especially pertinent to the questions of addressing cybercrime.

Cybersecurity (or its absence) can either facilitate or hinder cybercrime. For example, contextual aspects include the ubiquity of cyberspace, which tips the incentives to participate in crime in favour of the criminal (Giles, 2010) since all that is required is a speedy Internet connection and computer. The problem of spam perhaps personifies this. Sending huge quantities of spam is very low cost and it only requires one recipient to respond for the spammer to have turned a profit. The absence of cybersecurity may also provide the opportunity – for example in poorly secured products whose vulnerabilities are subsequently exploited (e.g. via so-called "zero-day" exploits).[16]

As we have seen earlier, different types of cybercrime can exploit different types of weaknesses – of a technical, organisational and human nature. This reflects an understanding that cyberspace (the environment in which cybercrime can occur) is actually a complex socio-technical system and although based around a man-made Internet infrastructure, is more than the sum of its parts.

Concrete examples of types of cyberinsecurity include Internet users running unsecured wireless networks and un-patched home PCs; banks with poorly secured and unencrypted databases of customer records, bank accounts and credit card numbers; software companies producing insecure code and web-hosting firms running servers with lax security. There are thus legion ways in which facets of cybersecurity impinge upon and create (or reduce, or remove) opportunities for cybercrime.

More specifically, these facets of strong or weak cyber-security can be attributed to different layers. We present below an analysis based on a simple taxonomy – at the

[16] A zero day exploit is where a vulnerability in a piece of code is exploited very rapidly after it is discovered and before the software manufacturing company has an opportunity to prepare and issue a patch

individual, organisational, national, market and international level and point to how these different types of actor can improve or hamper cybersecurity.

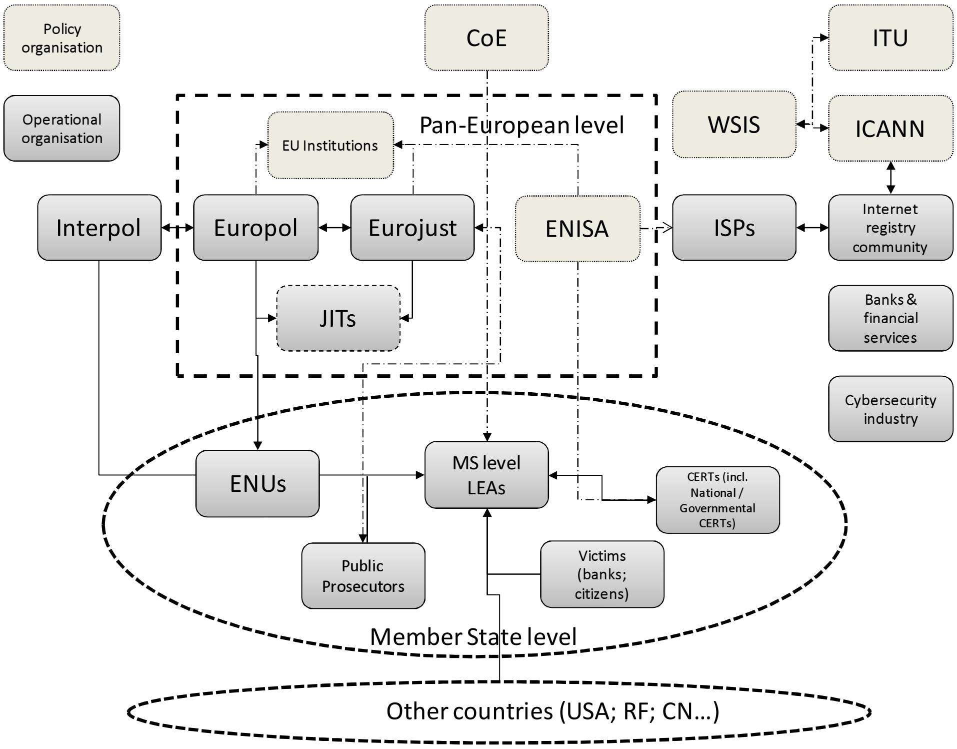
- **Individual** – at the individual level, aspects of cybersecurity which may affect cybercrime come down to the question of user responsibility, skills and awareness. To a certain extent, individuals may act irrationally and behave irresponsibly but as the Neighbourhood Watch example illustrates, also has the potential to improve security when a threat against a community can be determined. The question of the way in which fraudsters exploit psychological traits is important in this regard. For example, "phishing" works on the basis that a user trusts an important-looking e-mail from a financial institution. Similarly, with remotely facilitated scams such as romance scams or advance-fee fraud letters the context and other emotional factors may cloud judgement, leading individuals to trust or take decisions where normally they would refrain (Anderson, 2010).
- **Organisational** – across organisations the lack of security may present opportunities that criminals can exploit. Equally, organisations which take security seriously by for example, implementing effective security procedures and monitoring them, or ensuring that senior decision-makers have an adequate understanding of security may be able to help improve cybersecurity. This could include absent or poor system administration skills (which leave computers un-patched), low understanding of the risks by senior management (resulting in the security personnel being under-resourced) and poor engineering skills, which leave security as a final priority in the development of systems (Gordon, 2006).
- **National** – at national level, governments may be more or less prepared to initiate policy mechanisms to provide for cybersecurity (Dunn, 2006). This could include regulation (where appropriate) to compel certain activities, actions or support to development of cybersecurity capabilities (in for example, relevant government structures or via the establishment of national/governmental CERTs). Governments may also be responsible for neglecting cybersecurity by failing to implement certain policies or via other measures for example failing to implement specific laws.
- **Market** – at market level a number of factors affect cybersecurity, including the incentives operating on private-sector firms to produce better, more secure software code; take security seriously in system administration tasks; raise awareness amongst subscribers, users, customers and employees about risks; and share information on threats, vulnerabilities and concerns between themselves and law enforcement (Anderson, 2001). The question of information-sharing and exchange is particularly pertinent – law enforcement may be highly constrained by what information it can disclose since that could compromise an investigation, whilst firms are reluctant to indicate to law enforcement the extent of incidents because they either do not know the full extent or they fear that law enforcement involvement may either result in reputational damage (by publicising a breach, for example) or business interruption (if law enforcement needs to seize servers or data).
- **International** – at international level, efforts to address cybersecurity are undertaken between nation-states from within platforms such as the World Summit on the Information Society (WSIS), Internet Governance Forum (IGF) and International

Telecommunications Union (ITU). In addition, organisations such as the Internet Corporation for Assigned Names and Numbers (ICANN) and Regional Internet Registries (RIRs) play an important role at this level. Considerations to countries adopting cyberspace rules of the road are appearing, such as with the US international cyberspace policy, the announcement that next year the EU will publish its own cyberspace strategy and efforts at the London Conference in November 2011 to start the process of agreement on "norms" for cyberspace (what constitutes acceptable behaviour of nation-states in cyberspace) (BBC, 2011). However, confusion and poor co-ordination between governments at the international level may result in poorer cybersecurity where issues (such as the resilience of the Domain Name System) are left unaddressed.

3.1 Who is responsible for cybersecurity?

Any analysis of the role that cybersecurity plays within cybercrime should begin with an understanding of the range of different types of organisation that are involved. Facilitating and improving support to tackle cybercrime (such as a possible future ECC might be expected to provide) is ultimately one aspect of a much broader range of activities, involving, crucially, a range of organisations outside the criminal justice system such as communication service providers and financial institutions. . Aside from police and law enforcement agencies (about which we provide information from 15 European Member States in the next chapter) there are a host of other types of organisation across the public and private sector that are important. For example, we present below a generalised schematic of the different types of stakeholder involved in operational aspects of addressing cybercrime.

Figure 3.1 Relevant stakeholders involved in cybercrime aspects of cybersecurity



Source: Study Team

We provide a concise summary of the main types of organisation below. We list them to give an overview of the sheer number and complexity of different types of organisation involved in cybersecurity. They are relevant in any consideration of both the scale and nature of the phenomena (since many of these organisations may be considered as directly or indirectly responsible for levels of insecurity which provide opportunity to cybercriminals). Furthermore, an appreciation of the type organisations is important in order to arrive at a nuanced view of the complexity of addressing the issues at European level. This is particularly the case when understanding relationships between the public and private sectors.

Public-sector stakeholders

In the public sector these include government departments that may set national policy relating to cybersecurity. European examples include the Agence nationale de la sécurité des systèmes d'information (ANSSI) in France, the Dutch NICC (National Infrastructure against Cybercrime) the Bundesamt für Sicherheit in der Informationstechnik (BSI) in Germany and the Office of Cyber Security and Information Assurance (OCSIA) in the UK. In Slovenia progress is underway to establish a National Cyber Security Centre (NCSC). These high-level national organisations are relatively new. They usually attempt to bring together input from a range of other public organisations and agencies including law enforcement, defence, intelligence services, economic affairs, interior and telecommunications departments or ministries. Some have lesser or greater contact with the private sector, specifically infrastructure firms, hardware and software providers, communication service-providers and financial institutions.

Such organisations have prepared different cybersecurity strategies.

- The 2009 Cyber Security Strategy of the United Kingdom established the Office of Cyber Security (now OCSIA) and the Cyber Security Operations Centre (CSOC) (Cabinet Office, 2009).
- France, similarly, has elaborated their 2011 *Défense et sécurité des systems d'information Stratégie de la France* (Defence and Security strategy for strategic information systems of France) (ANSSI, 2011).
- Similarly, The Netherlands recently released "National Cyber Security Strategy (NCSS) – Strength through co-operation" (Ministry of Security and Justice, 2011).
- In Germany, the 2011 Cyber Security Strategy noted that the IT Planning Council would have a stronger role in facilitating the establishment and functioning of CERTs (Bundestag, 14/8/2009).
- The Cyber Security Strategy of the Czech Republic for2011–2015 was published in June 2011 (Parlament České republiky (2011).

Many European countries are now setting up specific national/governmental CERTs (Computer Emergency Response Teams). According to the European Network Information Security Agency (ENISA, 2010), there were 23 national/governmental CERTs in Europe in 2011. Examples include GovCertUK and GOVCERT.NL in the Netherlands. CERTs may be seen as "digital fire brigades", aiming to support the detection, mitigation and restoration of different types of security problems (ENISA, 2011a). CERTs are covered more in detail below.

Aside from law enforcement, other organisations include interior ministries and intelligence agencies. Whilst law enforcement and intelligence agencies remain separate for reasons of transparency in accordance with democratic principles, in reality a certain degree of operational co-ordination takes place, in particular where serious and organised crime poses a severe national-security threat. Such co-operation also exists with respect to investigations of terrorism, for example. In certain limited circumstances, there may be calls for co-ordination with military or defence organisations, again depending on the severity of the perceived risk.

Outside of these specialised communities there are other members of the criminal justice system – most notably public prosecutors, courts and the judiciary – also considered in the remainder of this report (particularly as they link to supporting joint investigations and often form a crucial link in chain from intelligence to prosecution). Unlike the intelligence agencies and some law enforcement approaches (which focus on disruption and dismantling of criminal networks), the judicial authorities have successful prosecution as an overriding objective.

Data protection authorities (DPAs) or independent supervisory authorities governing data protection are also important. Although they have a specific role (in a European context) that is the protection of the fundamental right to privacy of personal data, by monitoring the application of security measures by organisations using personal data ("data controllers") they can help to reduce organisational and procedural vulnerabilities, thus making it harder for cybercriminals to exploit personal data. For example, if an organisation is in breach of certain obligations under data protection legislation (for example, by failing to abide by provisions concerning security measures on individuals' personal data) then the risk that this might be copied out of the organisation by an organised criminal element may increase. Some DPAs have enforcement powers. The role of DPAs is becoming increasingly important as personal data is, according to the OECD, the new "oil" of modern economic growth and, as we have seen previously, an important commodity in the criminal underworld.

Other relevant public-sector organisations include regulatory authorities in specific sectors such as telecommunications or finance which may exert power over private-sector organisations responsible for supporting cybersecurity. A good example of this is in respect to regulators who may issue, review and revoke licences for providers of publicly available electronic communications networks. Their rules may contain specific provisions that the regulated parties must maintain appropriate levels of security to guarantee service. Other examples include financial regulators who may require financial institutions to conduct fraud checks in order to maintain a view and appreciation of operational risk.

Private-sector stakeholders

The private sector is often mentioned in discussions about cybercrime but care is needed to understand the different types of private-sector stakeholders and what role they play, since the motivation and character of their contribution to cybersecurity varies.

Many argue that the challenge with cybersecurity is that the private sector would appear to operate under misaligned incentives to take cybersecurity seriously. Ranging from poorly designed software to unwillingness to disclose information, private sector motivation to act is often on the basis of trying to fix the symptom rather than addressing root causes, which would cost more money or reduce revenue – for example, imposing further security measures on e-banking customers may result in some turning away or choosing different banking (on the basis that there is too much inconvenience associated with the security measures) (Anderson *et al.*, 2008).

Private-sector players, most notably financial institutions, ISPs and security-service providers have a more accurate and up-to-date picture of the extent of vulnerabilities, botnets and malicious software, not to mention actual incidents. It is commonly understood that regulatory intervention is required to force them to report incidents, which they might otherwise keep confidential for fear of reputational damage. This is particularly the case for the financial sector where trust is the key underlying characteristic of the market. An analogy may be made that if customers see police cars parked outside a bank, for example, then trust in the institution may be negatively affected, based on the perception that the institution is unsecure (Ko, 2006).

Other challenges common to the sector include the pace of technological development within cyberspace, which can complicate law enforcement activities. Examples include the use of cloud computing, which makes the identification and seizure of data difficult

(Robinson *et al.*, 2011), and the transition from IPv4 to IPv6.[17] The broader use of IPv6 may serve to complicate the challenge of attribution by exponentially expanding the possible IP address space, making remote investigations difficult and further opening up the gap of attribution between law enforcement and cybercriminals.

Across the private sector those companies involved may be seen as directly or indirectly contributing to or inhibiting cybersecurity. Financial institutions, for example, may be both a source of useful intelligence to law enforcement (e.g. via fraud investigation teams co-ordinating with police forces) but also a challenge, since by refusing to exchange data on incidents, they hamper efforts to gather a more accurate picture of the phenomenon. Financial institutions may be victims themselves (as in the case of phishing) and may already "price in" fraud and abuse to their business models (much as grocery stores allow for shrinkage and are able to calculate the impact of shoplifting when predicting stock levels). Other examples of financial institutions that play a role are payment mechanisms such as credit card companies and both offline and online global payment systems (e.g. Western Union and Paypal). These latter companies in particular have come under criticism since by their nature they are seen as key to the realisation of the proceeds of cybercrime, either in payment of mules, for example, or in bringing proceeds of crime into the licit economy. Credit card companies in particular have begun to understand the role that they play in the phenomenon of cybercrime – witness the participation of American Express in the European Electronic Crime Task Force (EECTF) for example.

Other key players in the private sector are companies responsible for the design and engineering of the products and services used in cyberspace – the software, programs, apps and middleware that are used in laptops, tablets, smartphones, PCs, servers and important elements of the Internet infrastructure (e.g. routers). As Anderson (2008) points out, often the economic arguments for security come a poor second against time-to-market pressures or the desire to increase profits. Companies that manufacture poor software with flaws provide opportunity for those in the underground economy who construct or prepare the malware and exploits for these vulnerabilities. The question over imposing liability for software bugs has been discussed extensively by researchers and experts {Cusumano, 2004 #117}. Some have argued that from a legal standpoint this may prove difficult because without clearer indications of the financial liability to which software producers would be exposed, a regime would not have the desired effect. Another key aspect of software security is the problem of "zero-day" exploits – that is a vulnerability that is found and exploited before the vendor is aware of it. Some advocate full disclosure of such vulnerabilities because it forces software companies to take remedial action. However, many vendors argue that those exploits that are used by malware are actually years old – thus the problem is system administrators not patching systems and keeping security up-to-date (Keizer, 2011).

[17] As explained by the RIPE (European IP Networks) Network Co-ordination Centre "Internet Protocol version four, or IPv4, is a system of addresses used to identify devices on a network. IPv4 is the most widely used Internet layer protocol. IPv4 addresses are actually 32-bit numbers. This means that there are just over four billion possible addresses. Over time, however, it has become clear that more addresses will be required to ensure ongoing growth of the Internet. The IPv6 address fields are 128-bits."

Companies that provide hardware upon which the infrastructure runs are important, since vulnerabilities may give rise to opportunity for cybercrime to take place. Firms including Cisco Systems, Juniper Networks and Huawei manufacture the hardware (routers, switches and gateways) used in much of the Internet infrastructure. The cybersecurity implications in this sector include the extent to which flaws and vulnerabilities in middleware and hardware could be exploited by cybercriminals. In addition, firms have a role to play with respect to the global-level Internet infrastructure for example by enabling the deployment of Domain Name System Security Extensions (DNSSEC) or other tools to provide greater security in key cyberspace infrastructure such as the DNS system; Internet Protocol (IP) addressing; routing tables; various peering protocols such as the Border Gateway Protocol (BGP). Insecurities in these provide the opportunity for cybercrime to flourish.

Yet another important business sector is providers of public Communications Services Providers (CSPs) and Internet Service Providers (ISPs). They may be incumbent fixed-line operators, or mobile network operators, or cable companies offering Internet, voice and other audio-visual services (IPTV). Other types of communications services that may be provided include e-mail and access to Internet Relay Chat (IRC) services. ISPs generally operate on the "carrier principle" with respect to liability – namely that they offer carriage of data and are therefore not liable for content.. CSPs are normally further differentiated into back-haul providers providing transcontinental connectivity, and those in a metropolitan area; they may also be classified along the lines of retail, business or resellers and access or transit providers. Many CSPs do not own infrastructure – they may lease fibre from "dark" (unlit) fibre optic providers or rent infrastructure (e.g. mobile 'phone masts or spectrum) from others. Some of the larger ISPs may act as Autonomous Systems (AS) and agree to exchange traffic with each other at peering points, usually at Internet Exchanges (IX) – examples being Amsterdam Internet Exchange (AMS-IX) and London Internet Exchange (LINX) (ENISA, 2011b). CSPs with access subscribers may run abuse desks where subscribers can report content and in some countries this is required by law.

CERTs within ISP companies are regarded as one of the key stakeholders in any cybercrime effort. CERTs are tasked with formulating a response to information security incidents and sometimes interact with law enforcement if prosecution is deemed appropriate after an incident. CERTs are focused on problem-solving, for example getting the network back up, so their approach may sometimes be at odds with law enforcement particularly with respect to the preservation of evidence. The law enforcement objective may be to shut the system down in order to preserve evidence whilst the CERT will be trying to keep the system up and solve the problem. CERTs can take as input sources of data from their subscribers, who may report an incident or problem in addition to network and system monitoring, and feeds from other external sources such as security-service providers. CERTs often operate a system of workflow triage where problems are escalated depending on the severity and number of constituents affected. Some CERTs have been known to operate more sophisticated activities, for example, with respect to botnet infection, at least one CERT is known to operate a triaged process of informing the subscriber, if they connect via the ISP network, that their computer appears to be compromised (since the ISP can detect anomalies through the analysis of the volume and source/destination of IP traffic), pointing them to anti-virus products. If the subscriber persists in trying to connect with a compromised machine then he is placed into a "walled garden" which restricts the connectivity of the host to the broader Internet. CERTs work within constituencies which represent user groups or those whom the CERT serves.

In general, CERTs may be one of the following types:

- A CERT working within an ISP or CSP whose constituents (users) are subscribers to the service.
- A CERT for a specific product, e.g. a router or particular piece of hardware, whose constituents are the users of that product. The users of products may be private users or organisations.
- A CERT within an organisation such as a company, or government department, or ministry where the constituents are employees. University CERTs may also have students and staff as constituents.
- Finally, a new classification of CERTs is a national/governmental CERT, which is a CERT having a national role that aims to act as a contact point for Critical Information Infrastructure Protection (CIIP). National/governmental CERTs sit within a peer group of others but have a specific aim to co-ordinate responses to cyberattacks with a national implication (for example, attacks against critical Information infrastructures underpinning energy, banking or transport networks) (ENISA 2011a).

Content platform providers such as Yahoo!, Google and Facebook develop and provide services and technologies allowing for the production and dissemination of content. Such content might be from an established provider (for example, a newspaper) or it might be user-generated content (UGC) from users of the platform. Facebook, a social networking site (SNS), is perhaps the best case in point. Facebook has several billion users and has been likened to a microcosm of the Internet in respect to the types of activity present on its network. SNSs are important to consider because they can provide evidence of criminal activity. In addition, they are a useful source of intelligence for cybercriminals and law enforcement alike. Cybercriminals use SNSs to gather information to help social engineering attacks (ESET Threat Blog). Conversely, law enforcement can analyse information from SNSs to help track down cybercriminals.

Content delivery networks (CDNs) such Akamai operate to make content (from content providers such as media companies) more easily available by hosting content at points on the Internet infrastructure that are highly accessible – usually Internet Exchanges and peering points – to access ISPs. CDNs are relevant since they provide another layer of the dissemination of content and facilitate easier access to content by Internet users.

Hosting companies offer opportunities to build, deploy or run a website or other forms of publicly or privately accessible online service. This is done by provisioning server space and bandwidth for leased access to the host. Many hosting companies now offer off-the-shelf packages including applications and complex remote-management systems, permitting the customers to adjust a variety of parameters of how the site operates, via a web-based interface. Hosting may include space on servers shared with other customers or it may be just hardware present in a telecom-hosting environment. Telecom hotels provide physical infrastructure (building, heating, air conditioning, security access control, etc.) if customers wish to deploy their own servers. So called bulletproof hosters (advertised as such on the criminal underground) are seen as a particular nuisance since they are immune to law enforcement agency (LEA) requests to shut down services – either deliberately or maliciously choosing to ignore or thwart such co-operation. According to reports, bulletproof hosters differentiate their offerings to the underground economy by indicating how immune (available) the hosting services will remain (in terms of length of time) before law enforcement action.

Confounding the separation of the last three types of private sector player are those companies offering cloud computing services[18] – which may be broadly considered as a combination of content delivery, hosting and communications services. Cloud service providers may offer user applications and services (e-mail, sharing of documents), networks (such as SNSs) but also more complex applications (databases, hosting and application environments) storage space, processor capacity (CPU cycles) and even hardware (dynamically reconfigurable combinations of processors, memory, storage and infrastructure) in the so called "Hardware as a Service" (HaaS) model. Cloud computing service providers include companies such as Google and Microsoft, but also Amazon and others offering hardware-based solutions.

Security product and service providers are another important link in the cybersecurity chain. Companies including McAfee, Symantec, PandaLabs, RSA Security and others develop security and anti-malware products including anti-virus tools, firewall software or other mechanisms. Other software firms may also work in this area – for example, Microsoft releases its Security Intelligence Report, derived from malware detection software running on Windows-based computers, which allows the company to perform analysis of the number of malware detections on those computers. Security firms, particularly anti-virus companies, often run research and development laboratories (e.g. RSA's FraudAction Research Lab) which deconstruct malware in order to better understand it and provide signatures allowing detection. These signatures are then disseminated to users of the software so that they can remain protected. Subscribers usually pay an annual subscription to receive these signatures. Other companies may run or manage sensors on networks which can be used to collect information on vulnerabilities, threats, etc., which can be further analysed. There is also an emerging type of Internet security and research organisation (e.g. Team Cymru Community Services, which is a non-profit organisation) that analyses cybersecurity data.

A wealth of other for-profit and non-profit organisations and projects is emerging into a cybersecurity "eco-system" aimed at using the increasing volumes of security data/metrics now available to help or encourage better cybersecurity practices within organisations. For example, the commercial Abusix project co-ordinates the exchange of abuse-related reports between ISPs. Projects such as Spamhaus maintain blacklists of known sources of spam and work with ISPs and LEAs to identify and deal with spammers. Similar activities are underway with botnets – for example the Anti-Botnet Advisory Centre run by eco, the

[18] Cloud computing is defined by the US National Institute for Standards and Technology (NIST) as: follows "Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."

German ISP association. Other examples include the Swiss Abuse.ch site which provides publicly available blocklists containing known command-and-control domains and IP addresses in botnets. These organisations and projects frequently use network sensors to identify new malicious command-and-control domains, IP addresses and servers to keep databases regularly updated. This is so that ISPs, other companies and browser developers can in turn keep their signatures up-to-date. ISPs may be able to use these data to prevent access by compromised machines run by subscribers to command-and-control servers, preventing them from participating in botnets.

The Co-operative Association for Internet Data Analysis (CAIDA) is another interesting organisation in this cybersecurity eco-system. CAIDA conducts analysis of the overall "topography" of the Internet, highlighting topographical nuances of the Internet that may provide opportunities for malicious activity. An example is the so called "dark-web" where there are unallocated or unused IP addresses.

Companies also offer independent testing of cybersecurity products – examples include West Coast Labs, ICSA Labs or AVtest.org which analyse the efficacy of anti-virus signatures.

Predictably, these resources have themselves come under fire from cybercriminals – both Spamhaus and Abuse.ch have been targeted in various ways as an attempt to undermine their credibility and the integrity of their data (ESET Threat Blog).

Non-Governmental Organisations

There are also a number of important Non-Governmental Organisations (NGOs) that play a role. Perhaps chief amongst these is the Internet Corporation for Assigned Names and Numbers (ICANN) with its Internet Assigned Numbers Authority (IANA) function.

ICANN is at the heart of Internet governance since via its IANA function it manages the framework for the operation and assignment of Internet Protocol (IP) address space to Regional Internet Registries (RIR). The RIRs (of which there are several, with RIPE being the European RIR) then assign blocks of IP addresses to others, which can be national registries (e.g. Nominet in the UK) or directly to organisations. ICANN and the RIRs work on the engineering-orientated principle of "consensus and running code" and have a grass-roots (non-hierarchical) form of governance, driven by the engineering-led character of participants, who often work for ISPs and other organisations involved in the operation of the Internet infrastructure.

The RIRs thus play an important role in helping to fight against cybercrime, since they may be seen as stewards of the IP addressing system and set policy (by this consensus method) for such crucial initiatives as deciding how much data should be in a domain name registration, the transition from IPv4 to IPv6 and so on. Indeed, there has been an ongoing initiative to clean the Whois database (the resource used to match IP addresses to domains, often used by law enforcement as an aid in investigations). Latterly, ICANN and Interpol have signed a Memorandum of Understanding in order to facilitate greater co-operation (New Legal Review).

Other important NGOs of specific relevance include such organisations as the International Association of Internet Hotlines (INHOPE) and participants of the Safer

Internet Programme, which run reporting points for illegal content (mainly aimed at online child abuse material).

There are also informal bug-hunters (technical experts who find problems in software that can be exploited and then disclose this information – either immediately or under a policy of responsible disclosure) to software firms or others. For example, Facebook recently announced that it would institute bug-hunting bounty via its Bug Bounty initiative – that is to say anyone discovering a vulnerability in its systems would receive a reward (Mills, 2011).

Other grass-roots initiatives include volunteer leagues such as the Estonian Cyber Defence League and vigilante groups such as Perverted Justice (Canoe.ca). Vigilante groups in particular come in for much criticism from law enforcement for muddying the waters of enforcement and addressing criminal activity, compromising investigations and making prosecution difficult.

Finally, there are examples of partnerships and multilateral organisations such as the Messaging Anti-Abuse Working Group (MAAWG) the Anti-Phishing Working Group (AWPG) and the International Cyber Security Protection Alliance (ICSPA). This last organisation is relatively recent and is a not-for-profit public–private organisation consisting of a law enforcement organisation, security service providers and a credit card company. The mission of the ICSPA is to channel funding, expertise and assistance directly to law enforcement cybercrime units.

3.2 Conclusions

This chapter has provided a summary of some of the most relevant aspects of cybersecurity pertinent to cybercrime and the possible work of the ECC. Cybersecurity is a much broader field involving, for example, consideration of the integrity of supply chains or innate vulnerabilities in information technology. This chapter has detailed the public- and private-sector players and some of the main issues of cybersecurity as they relate to the challenge of addressing cybercrime. There may be an inherent paradox however, in this analysis. If efforts to improve cybersecurity were more successful and cybersecurity was taken more seriously – resulting in fewer vulnerabilities and more secure system administration, then perhaps there would be less work for law enforcement to do. Addressing these simpler and more tractable root-cause aspects might free up law enforcement to focus on the persistent, motivated cybercriminals who pose a more serious risk in terms of their capacity to cause economic and psychological damage.

PART II

CHAPTER 4 Findings from the Member State interviews

This chapter sets out the emerging findings from the 15 Member State interviews.[19] The purpose of these interviews was to gather descriptive information about the law enforcement response to cybercrime in each country. The interview was semi-structured; this meant that we asked the same questions of each interviewee, but left scope for interviewees to add other information which had not been covered in the interview guide. The information reported in this section is based on information gathered in the interviews only, and has not been checked against other information sources. Nonetheless, the expert interviews represent an important and informative data source in and of themselves. More information on the methodology can be found in Appendix B.

In each of the 15 case-study countries we spoke with senior managers in some of the main law enforcement units dealing with cybercrime, generally one per country. This reflects the law enforcement focus of the study, and the fact that our sample was drawn from Member State representatives participating in the European Union Cybercrime Task Force (EUCTF). The time and budgetary constraints of this study meant that we could not speak to other law enforcement organisations who may have had complementary roles. For example: in Italy we interviewed individuals from the Postal and Telecommunications Police and not the Carabinieri or Guardia di Finanza (Financial Police); in the UK we did not talk to the Police Central e-Crime Unit (PCeU) of the Metropolitan Police. Further, in virtually all Member States we were told that other national and local agencies and other government departments had a role in the response to cybercrime. For example, in France the counterterrorism unit and the Agence nationale de la sécurité des systèmes d'information (ANSSI) were reported to also play a role. Our interviews did not extend to these organisations.

The cybercrime units included in our sample differed considerably in terms of their size, their position within the national law enforcement landscape, and their mandate.

Some of the units had evolved from more informal capabilities or arrangements for dealing with computer-related crime which had been established in the late 1990s, or the early

[19] We used a range of criteria to help support our selection including GDP, numbers of people online, total population and rankings from Microsoft's Security Intelligence Report. All data was for 2010.

2000s. Some had been created much more recently, for example Finland arrived at its current situation in 2009, the same year in which Slovenia set up their unit.

4.1 Organisational structures

Many of the “high-tech crime” units we visited were part of an Interior Ministry unit dealing with fraud and economic crime – for example, Belgium’s Federal Computer Crime Unit (FCCU) which sits within the Economic and Financial Crime unit of the Federal Judicial Police, the Romanian unit which is sited within the Ministry of Administration and Interior, and the Irish High-Tech Crime Unit which sits under the Fraud Investigation Division.

Others were in national criminal intelligence bureaux, for example the Polish Centralne Biuro Ĺšledcze (CBĹš), (Central Bureau of Investigation), the Finnish unit in the Keskusrikospoliisin (KRP) (National Bureau of Investigation) and the Dutch Korps landelijke politiediensten (KLPD) (National Police Services Agency). Most units in such national criminal intelligence bureaux were situated within administrative hierarchies which were addressing different types of organised crime, such as drugs and people trafficking, weapons, terrorism and broader economic and financial crimes.

The UK was the only unit which had a separate role reporting directly to the Home Secretary (equivalent to Minister of Interior).

We found a number of units that shared resources with other units. Mainly this focused on forensics capability supporting other types of crime or, more specifically, units dealing with the exploitation of children where the high-tech crime centre would be asked to provide support (for example, through wiretapping). This was the case in Germany (which has a federally structured policing and criminal justice system) in respect of the Bundeskriminalamt (BKA) Department KI – Forensics and SO 13 Child Exploitation. Finland was also an interesting case-in-point since the computer-crime capability was spread in what was intended to be a matrix structure across three Directorates (Intelligence, Laboratory and Investigations) of the National Bureau of Investigation serving a range of different organised crime commodities.

Some of the units we consulted were necessarily reflective of the unique nature of law enforcement structures in the country. For example, in France, we visited the OCLCTIC (Office Central de Lutte contre la Criminalité liée aux Technologies de L’ Information et de la Communication) – part of the National Police, in addition to representatives from the Gendarmerie. In Italy we spoke to representatives from the Polizia Postale e delle Comunicazioni (the Postal and Communications Police), which is part of the National Police; in Spain we spoke to officers from the Cuerpo Nacional de Policía (CNP) (National Police Corps), one of the two main police units (in addition to the Guardia Civil). The National Police is responsible for policing in major urban areas whist the Guardia Civil is responsible for policing rural areas. Broadly, this arrangement was also found in France.

Other units such as Sweden’s Cyber Unit are part of the highly centralised police force and can exercise a great deal of control over local police authorities. The Centralkriminalpolisen (National Bureau of Investigation) in Sweden is a centralised unit dealing with serious and organised crime. Similarly, the PCP in Italy can exercise a strong degree of control over nationwide resources, a fact that was reported as being unique.

Another feature of some of the units we visited was of change. Some units such as Slovenia or Romania described themselves as emergent and having been set up relatively recently and therefore still in a period of "bedding in". Others such as the UK or the Dutch High-Tech Crime Unit were undergoing significant organisational restructuring. The UK in particular was of interest since the Serious Organised Crime Agency (SOCA), with the forthcoming integration into the National Crime Agency, was in the process of developing a National Cyber Crime Centre (as part of the Government's Cyber Security Strategy, a revision of which was published at the end of 2011).

4.2 Mandate and focus

Breadth of mandate

Information gathered during interviews indicates that a small minority of the national units visited by the research team focuses *only* on categories of cybercrime relating to the confidentiality, availability and integrity of computers as defined in the Council of Europe's Budapest Convention. Belgium's FCCU, the BKA in Germany and SOCA in the UK had a specific focus on crimes such as on e-banking fraud, hacking and crimes where data or data systems are the target.

Most of the units we visited had some mandate also to deal with computer-facilitated crimes or any crimes that had a computer element (for example via provision of forensic support).

For example, the mandate of the Italian Postal and Telecommunications Police included monitoring online betting and gambling as well as responding to online child exploitation. In Spain, in addition to dealing with phishing and hacking, the unit had, for example, had a group which supported the investigation of illegal car-racing, on the grounds that videos of the races were posted online (interviewees did not elaborate on the form the support took). They also were involved in responses to the sale of narcotics on the Internet. In France the mandate was defined as any criminal activity publicly visible on the Internet. Finland's unit has been asked to follow-up on tracking terrorists and gathering intelligence on serial killers and "lone wolf" suspects.

This broad focus was partly confirmed in discussions with industry (for example Facebook), who indicated that their interactions with law enforcement often involved requests for information on suspects or where someone had posted their intention to engage in criminal activity).

This finding that national units have broad and diverging remits could be relevant to pan-European responses to cybercrime, in particularly responses in which peers from national units gather around a table – since there needs to be clarity on what is being discussed. Care would need to be taken when cybercrime is being discussed to define exactly what the understanding of each participant is, lest actions be taken that may be a disproportionate response to particular types of criminal behaviour, for example.

Discretion to investigate and take on cases

Some units, for example those in Slovenia and Belgium, could only intervene on request from their regional or local units, while others had a proactive stance and could take up investigations on their own discretion.

In some cases (such as in France, the UK and Holland) the units could exercise a degree of discretion as to which investigations they pursued (termed by the BKA as: "know, not act"). In others (Germany, most notably, but also Poland and Cyprus) it was reported to us that the police were legally obliged to follow-up on each and every complaint.[20]

The implications of this, particularly with respect to high-volume computer crimes (e.g. phishing), are that a strict interpretation of the national legal frameworks would risk the police being inundated with complaints from compromised computers acting as part of a botnet that they are obligated to follow up. This was noted specifically by the BKA due to the unique legal framework of German criminal law.

Strategic approaches

Findings from the interviews suggest differences in the approaches taken in different national units.

One the one hand, Belgium, the UK, Germany and to some extent Spain tended to focus on high-level strategic threats, and had long-term aims and objectives. For example, SOCA in the UK takes a "harm-reduction" approach (which is set out in legislation). This means that rather than focusing on prosecution or sentencing as the key outcome, the unit concentrates instead on such aims as disruption, intelligence-gathering and focusing investigative efforts on those groups and individuals who are causing the most harm.

On the other hand, there are countries that did not focus to *such an extent* on these long-term and strategic goals. This is not to say that this type of thinking did not occur in those units; on the contrary, almost all interviewees told us that prosecuting cybercriminals was not their only goal and that prosecuting one difficult case might be "worth" more than a simple case against a low-level criminal. For example, the interviewee from the Swedish Cyber Unit mentioned that one factor taken into account when deciding whether or not to take on a case referred by a local police force was whether the national unit could "learn something" from that case. However, the units in the UK, Germany and Belgium dealt exclusively with highly organised, serious criminals and cases that were of long-term strategic importance, whereas other units in other countries worked on a range of cases.

Thus, there do appear to be differences in the strategic focus of different units across the EU. One explanation for this is simply the differing culture and remit of the Units – SOCA in the UK, for example, has its "harm-reduction" approach written into legislation, and this guides its strategic approach.

[20] However note § 152 StPO of the German Criminal Code of Procedure – only true if there are sufficiently concrete elements of proof

4.3 National and local collaboration within Member States

Interviewees described to us the extent to which local or provincial police forces also had specialist skills in cybercrime, and how their national units worked with local units. Their responses were inevitably linked to the administrative and organisational structures of the law enforcement authorities in each of the countries. For example, in Germany, which has a federal system where each *Länder* has its own police force, the High-Tech Crime Unit in the BKA has developed a model of standing collaboration with each provincial police force. (Interviewees from Germany reported that the *Länder* were also in the process of setting up specialist units). Towards the other end of the spectrum, Cyprus has just one police force made up of six geographical divisions, and all cyber investigations are referred to the national-level unit for investigation.

Occupying a mid-way position on a scale of collaboration between local and national cyber units, Finland has 24 police districts and each district has between one and three forensic specialists as well as other police officers knowledgeable about cybercrime but who do not work exclusively on cyber.

In Italy, in additional to the national unit, the Postal and Communications Police has 20 regional offices whose staff includes engineers and technical specialists. Interviewees in Italy described a situation in which, compared to the UK where SOCA must work with 42 police forces, the head of the PCP has officers across the country in provincial units who are under his direction and control – which we were told facilitated smooth working across the country.

Even in smaller countries, such as Slovenia, we were told that there were police officers with cybercrime capabilities spread across regional units and in the major cities.

4.4 Resources

Human resources in the national units

In interviews we asked about the number of full-time equivalent staff working in the national units, and in any regional units. The figures provided are set out in Table 4.1.

For some interviewees it was difficult to provide an exact answer as to how many law enforcement officials worked on cybercrime in the country. In some countries, some of the staff who worked in the cybercrime field also worked in other crime areas (this was the case in Cyprus). Another complicating factor was that those undertaking cybercrime-related tasks at the regional or local levels might head a team of investigators or detectives who were non-specialist officers, but who had undertaken some specialist forensic training.

Table 4.1 Overview of number of people working in Member State cybercrime units and in local units, as reported by interviewees

Country	Number of full-time equivalent staff working on cybercrime in the whole country*	Number of full-time equivalent staff working on cybercrime in the national unit*	Officials in national unit per head of population**
Belgium	249	33	1 / 328,482
Cyprus	–	13	1 / 61,298
Finland	At least 24	29	1 / 183,666
France (National Police)	298	50	1 / 1,287,383
France (Gendarme)	250	24	1 / 2,682,048
Germany	At least 100	43	1 / 1,907,032
Ireland	–	15	1 / 296,669
Italy	1966	144	1 / 416,980
Luxembourg	Unknown	10	1 / 49,350
Netherlands	Unknown	30	1 / 549,526
Poland	Unknown	26	1 / 1,466,764
Romania	170	28	1 / 767,808
Slovenia	45	7	1 / 290,337
Spain (National Police)	182	46	1 / 996,265
Sweden	250	30	1 / 308,545
United Kingdom	Unknown	104	1 / 600,000

* Figures provided by interviewees

** Source: Eurostat

The numbers of staff reported in Table 4.1 broadly mirror the police force strength in each of the countries.

Seniority and background of staff

Evidence from the interviews suggests that the vast majority of units were staffed by a mix of police officers/law enforcement professionals and specialist technicians, engineers or computer scientists. For example, in the Dutch HTCU the two senior advisors were civilians and there was a 50–50 split between technicians and police personnel.

An exception was Luxembourg which had eight staff and only two full-time police officers (the rest were civilians). One interviewee (Sweden) commented specifically on the value he perceived in having police officers, with additional specialist training, working in cybercrime; the background in "general" policing provided vital experience of how to run an investigation.

Our interviews revealed some ways in which different units had brought in specialist skills from outside their units: the Netherlands housed ten members of staff seconded from the private sector – specifically the financial services industry – who were working alongside law enforcement officers; the Irish cybercrime unit sourced at least some (if not all) of its technical specialist from the computer science department of University College Dublin; an interviewee from the Swedish high-tech crime unit also mentioned that his unit had collaborations with universities that provided support to the unit on specialised technical problems.

We obtained limited quantitative information as to the seniority and background of staff members.

Training of staff

Training of officers and other staff working in the field of cybercrime, and the related topic of the professional and academic backgrounds of staff, were raised in almost all the interviews. We discuss separately training provided *by* members of the units (see below) and concentrate here on the training of staff in specialist units.

Many of the law enforcement staff working in the units had no specialist background – they had undertaken the usual training processes to join and progress within the police. For example, in Cyprus we were told that all members of the unit had graduated from the Cyprus police academy. Interviewees from Belgium described recruitment into the unit from the ranks of police officers as well as some specialist recruitment directly into the unit from outside. Slightly differently, in Romania we were told that most staff were drawn from the police academy but that many had a background in law and IT. In the Netherlands, staff members joining the unit received basic training in investigations, legal requirements, and writing reports to be used in prosecutions and in court, etc.

Officers were described as then undertaking some specialist training on their reception to the unit – in topics including forensics, investigation and so on. In the time available for the interviews, we did not capture detailed information about the timing, content, location and frequency of training for staff working in the units.

The picture that emerges from the interviews is that seemingly each country provides its own specialist training for officers in specialist units – we are not able to comment on the extent to which the content of the training is consistent across countries. There is some involvement of the private sector and academics, in some countries on some issues. Additionally, all countries have the opportunity to tap into some international training resources – we were not able to learn the extent to which these opportunities are taken up.

This picture suggests that a training needs assessment – which CEPOL told us they were now undertaking – would fill an information gap about what training is provided across the EU. Only one training need or gap was explicitly mentioned: one country noted that the person in charge of feeding information into the Analysis Work File Cyborg (see section 4.6) did not have training in intelligence.

One training course about which we did receive a detailed account was the MSc in Forensic Computing and Cybercrime Investigation offered by University College Dublin (UCD). That institution also offers other programmes and modules which are only open to members of the law enforcement community. We were told that all of the staff in the Irish Hi-Tech Crime Unit had received academically accredited training at UCD. Three people from the Netherlands unit had also received this training. Undertaking this course results in an academic qualification.

Interviewees in Germany and Romania mentioned that training was or should be "continuous" and a long-term process.

Budget and financial resources

In relation to budgets, we can divide the case-study countries into those that had a defined budget for their unit, and those that did not.

In the former category, interviewees in the UK reported that the total annual budget for dealing with cybercrime within SOCA was €2.5 million (£2.19 million). The Swedish indicated their budget was €2.5 million a year.

In the latter category, Ireland, Spain and Romania (for example) reported that their units had no ring-fenced budget that they had to manage. These units could make requests for particular expenditures (for example, new equipment).

Some interviewees who had no fixed budget overall for the unit could specify amounts spent on hardware (e.g. forensic capabilities, IT systems, Network Attached Storage [NAS] devices), training (travel and subsistence to attend training courses, cost of purchasing the training, cost of delivering training).

Interviewees from the UK, Netherlands and Slovenia reported that funding for their units had been increased in recent years, reflecting increasing political interest in and the high priority of cybercrime within these countries.

Some units reported being on a lower scale of priorities than counterterrorism, for example. However, when this was explored in the context of the mandate as described above, it appeared that this was being driven to a certain extent by the push to expand forensic capabilities to service support for a number of other types of crime. As technology has pervaded criminal behaviour, in the same way that it has other areas of society, it forms an important part of investigative activities and is a potential source of evidence across practically every other crime commodity (e.g. homicide, assault, suicide, etc.).

4.5 Activities of the national units

Conducting investigations, gathering and analysing intelligence and undertaking forensics analysis and support were the three activities in common across all the units visited.[21]

Investigations

Conducting cybercrime investigations was one of the main tasks of the units we looked at. Most of the units had or shared responsibility for investigating cybercrime and computer-related crime. As described above (section 4.2) this was either on a reactive or proactive basis, some units provided only investigative support to local police forces, other initiated and ran their own investigations (e.g. SOCA in the UK).

[21] There were, of course, some exceptions. For example, the Swedish unit and the French Gendarmerie did not undertake any intelligence-related activity (probably on the grounds that other institutions undertake this, for example, L'Agence nationale de la sécurité des systèmes d'information (ANSSI) in France.

The role of the public prosecutor also differed across the countries. In some countries the prosecutor had to undertake pre-trial investigation and the police were an “arm” of the prosecutor. In other countries the police could undertake a significant amount of work to prepare a case before placing it in front of the prosecutor.

A range of tools and methods were noted as being used to support investigations including the strictly controlled use of covert investigators, wiretapping and other forms of online monitoring (e.g. random Internet searches). The use of undercover investigations was reported a number of times in regard to investigating online child exploitation since many of these criminal networks were resorting to more stringent methods to “vet” members.[22]

Another crucial part of investigations is co-ordination with other peers across the EU and elsewhere (particularly the United States, Russia and the former Soviet Union). Here we discovered challenges in the speed of obtaining action via Mutual Legal Assistance Treaties (MLATs) and “letters rogatory” (a formal letter of request sent by a judicial authority).

Investigations can also result in the blocking of websites. This was described as an important and frequently used tool by the Italian CNCPO (Centro nazionale per il contrasto della pedopornografia or the National Centre Combating Online Child Pornography). We were told that in Italy a ministerial decree obliges ISPs to block child pornography sites within six hours. Other units also discussed filtering and blocking systems as a way to render inaccessible websites hosting illegal content.

Intelligence

Three broad classifications emerge from interview findings about the role of intelligence in the national units.

In one category, we can place SOCA in the UK and the FCCU in Belgium – both of these units had the production of intelligence as a key aim of their agency, and were tasked by government to provide information to fill in an intelligence picture. Finland also had a dedicated intelligence function within their national unit, and could probably be placed within this group.

At the other extreme, we can identify units which were described by interviewees as having no or a very limited intelligence function (Cyprus, Luxemburg, Slovenia, Sweden). Of course, these units might share information with other parts of the national law enforcement community and contribute to intelligence in this way.

Thirdly, are countries who do not have their own intelligence function, but who actively feed into a national intelligence function (Spain).

In those countries that did have an intelligence capability, it was reported in a number of instances that the technology (for instance, national-level intelligence databases) had still to catch up with cybercrime since the current crop of intelligence databases did not have the capability to store cybercrime-specific data (e.g. IP addresses). A further part of the

[22] For example, in order to gain access to some online communities for the sharing of illegal images, prospective members may have to submit images to prove their authenticity. This creates a challenge for undercover officers since this would be in and of itself illegal.

intelligence-gathering picture revolved around co-operation with other stakeholders, most notably the private sector (mainly being financial institutions and CSPs).

4.6 Contributions to relevant European-level intelligence databases: AWF Cyborg, AWF Terminal and AWF Twins

Not all interviewees commented on their national unit's contributions to these databases.[23]

The Slovenian unit reported that it was not yet contributing to Cyborg – partly because intelligence-gathering and analysis was undertaken in another unit of the police, and there was debate about which department should contribute data to Cyborg.

Luxembourg contributes to AWF Cyborg but since the unit is not a permanent member of Cyborg, this is done on an ad hoc basis when officers judge international co-operation is an advantage. The interviewees mentioned that they do not always receive information in return.

Sweden reports that one member of staff fed information to Cyborg, however, this staff member did not have specialist intelligence training (and this was combined with the fact that the national unit did not collect intelligence information itself).

Romania reported that they contributed to Cyborg, Terminal and Twins. Germany reported that they have an observer basis on AWF Cyborg.

One interviewee raised some questions about the use of Cyborg. Firstly, this interviewee mentioned that for their country, it would require one full-time equivalent member of staff to manage the traffic to AWF Cyborg. Secondly, the interviewee raised a point about the capacity of countries to send large amounts of information over a Virtual Private Network (VPN). Thirdly, the interviewee raised the possibility that for Member States in which those dealing with cybercrime have a well-developed network of connections with law enforcement in other countries, there might be limited incentives to input information to Cyborg, when they can simply share information through bilateral, personal connections (this route avoids the need to seek formal consent from the information provider to input information to Cyborg).

Another interviewee mentioned similar concerns. One set of interviewees reported that they had been a big contributor to AWF Cyborg last year but this year has not contributed anything to the system.

On the other hand, interviewees from Cyprus reported that they found AWF Cyborg very useful. Europol had analysed the data they had submitted and launched two Joint Investigation Teams (JITs) based on this analysis. However, the interviewees from Cyprus commented that not all countries contribute to Cyborg, and that a potential problem is that the data submitted is analysed but that there is no operational capability within

[23] The following mentioned Cyborg: Netherland, Cyprus, Slovenia (mentioned Cyborg to say they do not yet contribute), Sweden, Finland, Belgium, Luxemburg, Romania, and Germany; Romania and Sweden mentioned Twins. Only Romania mentioned Terminal. Of course, because interviewees did not mention it in the interview should not be taken to mean that they do not contribute. In the limited time of the interview different interviewees focused on different aspects.

Europol to act upon it. This last point perhaps raises a question about the perception of Europol within Member States – namely that in this instance, Europol was perceived as having a mandate to conduct operations directly from such analysis.

4.7 Forensics

Units in Cyprus, Finland, Ireland and Italy, Luxemburg, the Netherlands, Romania, Slovenia, Sweden and the UK were among the many units who reported that forensics formed a major element of their activities.

In the Netherlands, for example, interviewees described their role as supporting other police units, including through buying new software, creating new software and figuring out how to solve forensic challenges.

Although Spain reported that the national unit was not responsible for forensics – which was instead undertaken by the technical section of the national police – the unit did have technical specialists who prepare forensic evidence for use in court.

We identified some commonality across countries included in our research concerning different "levels" of forensic capability required to acquire data to necessary evidential standards. At the most basic level, this involved the acquisition and recovery of active files on a Windows or Linux file system; at the second level the recovery of e-mail traffic logs. At the third level was the recovery of hardware (deleted/wiped data).

To a certain degree, this model of levels of forensic capability matched training requirements: a basic forensic skill would allow the imaging of a Hard Disc Drive (HDD), an intermediate level would permit the officer to rebuild a suspect's digital life (e.g. from e-mail or a web-browsing trail) and the most sophisticated capability would allow the operator to conduct real-time network forensics). A further aspect of forensic capability was in regard to the acquisition of software licences, which accounted for a significant part of the non-annual operating expenditure of units (between €200,000 and €300,000).

Backlog and workload

Several interviewees mentioned the possibility of backlogs in forensic case-work, and high demands for these services.

In Ireland, it was reported that the unit receives between 650 and 700 requests for assistance per year, and these vary in scope from examination of one computer to information about a child exploitation network with many members. On average, the unit examines 14 computers per case. They have the capacity to examine 400 cases a year on average, which means the unit has a backlog of work.

In Romania we were told that the forensics capability was limited and overloaded by the requests made of it. Slovenian interviewees reported a significant increase in computer forensics requests and the work of their unit, which interviewees attributed to an increase in awareness of capabilities and increase in staff.

As part of improving the workload, interviewees in Finland spoke of the need to improve the ability of local policy units to decide what needs to be sent to the national unit for forensic analysis. In Germany, the forensic unit is a separate department within the BKA, and interviewees commented that requests for forensics in "pure" cybercrime cases (as defined in the Budapest convention) competed with requests for digital forensics in cases such as murders or burglaries where evidence happened to be stored on computer. Forensic capabilities were often under pressure from conventional criminal cases where the investigators wanted to examine an electronic device found at the scene, or, for online investigations, where the investigators were attempting to build a picture of a suspect by piecing together his or her "digital life".

We found in some cases that cybercrime units dedicated the majority of their time to this kind of activity (e.g. in Slovenia, where only 80 percent of the forensic workload was for "true" cybercrime).

One interviewee discussed with the challenges of devising metrics to measure the future potential forensics workload. The size, quantity and variety of electronic devices that could be used for storage makes it difficult to estimate future needs with respect to forensic capability. One possible, and simple, metric was to look at the number of PCs within a country. The problem with that approach is the rise in cloud computing potential future decreasing levels of PC ownership and increasing ownership and proliferation of other devices such as smart phones, tablets and other Internet connected devices. An alternative metric is to base estimates on the number of disks to be imaged. The problem with that is that computers have multiple disc drives and the different ways of storing data which would make this task exponentially difficult (e.g. via thumb drives; GPS devices). Finally, it may be possible to measure workload/increase by the size of the disc, however, given that the cost of disk space is rapidly decreasing this may also mean that law enforcement has to invest in ever more expansive storage infrastructure to keep up.

4.8 Providing training

Many of the national units – including those in Cyprus, Italy, Luxemburg, the Netherlands, Slovenia, Spain and Sweden – provide some training to other parts of the law enforcement community, for prosecutors or for the provide sector.

For example, in Luxemburg staff from the unit provide a one-day training course in basic forensic capability to regional police forces on a yearly basis for a one-day period; in Italy we were told that the unit provides training in digital forensics in collaboration with private-sector providers of the forensic analysis software. In the Netherlands the KLPD provides training for technicians through ECTEG, and writes a curriculum for the regional police forces to follow yearly to maintain literacy in the basic cybercrime issues.

4.9 Running a reporting system/hotline

During interviews we asked whether or not there was a public-facing hotline for reporting cybercrimes. Several Member States had a facility for the public to report all types of crime (not just cybercrimes) online, including Spain, Sweden, Finland and Italy (www.commissariatodips.it). Ireland reported that there was a hotline specifically for cybercrime (http://www.hotline.ie/) but this was not run by the police, as did Romania (@frauds.ro).

In the UK, SOCA did not take crime reports, but SOCA might be passed information about crimes reported to the UK National Fraud Office. Similarly in Slovenia, a public reporting website had links to the economic crime unit, and they had an anonymous hotline for reporting child exploitation.

Interviewees did not reflect in depth on the value added by these hotlines. In countries such as Spain, a crime report must be signed by the complainant before it can be investigated – and we were told that in some instances individuals who had made a complaint were asked to attend a police station to sign their report.

Interviewees from Italy provided detailed information about the number of reports through their online police station. This information is reproduced in Table 4.2.

Table 4.2 Italian online police station statistics

On line police station	1 July 2009–30 June 2010	1 July 2010–30 June 2011
Information requests	7,962	14,668
Crime reports	12,475	14,018
Online complaint	5,769	10,586

Source: Italian PCP

The usefulness of such mechanisms was reported as being variable. This was reported (e.g. by Belgium) as being due to the quality of data provided by the witness and the complexity of distinguishing multiple reports of the same incident.

4.10 Research and development

The involvement of national units in research and development activities was raised in interviews with four Member States (Luxemburg, Slovenia, Spain and Sweden), although it could be the case that this is undertaken in other areas, but was not raised in interviews.

The message from these four countries was that they all worked to find new technological solutions to addressing emerging threats and problems. This involved: devising and testing new tools and techniques for investigation; testing new software provided by private companies for undertaking forensic analysis; research and development into the technical aspects of things like wiretapping. In Sweden, staff in the forensic laboratories (separate from the national cybercrime unit) conducted evaluations on newly-issued software.

Only staff of the unit in Luxemburg described research and development activities as being part of their core role. In Spain research and development activities by the unit were described as "ad hoc" – by which we understand that they responded to particular questions arising during cases. The Swedish interviewees said that they were constantly trying to find new ways to solve problems – and in this sense, perhaps their day-to-day jobs included an element of research and development.

4.11 Outreach and prevention

At least four of the national units visited undertook preventative work, and "outreach" activities to educate and raise awareness with members of the public and specific audiences such as businesses, teachers, schools, parents and so on.

It was reported that the majority of outreach and preventative activities were undertaken in collaboration with the private sector or NGOs – for example, this was the case in Finland (working with NGOs) and Ireland (harnessing the support of the private sector). In Sweden (and this is likely to be the case in other countries), giving presentations in schools was the role of local police forces, rather than national units.

We saw a varying extent of collaboration and outreach activities. This ranged from "social media police" in Finland to sophisticated partnership schemes reported in the UK, Netherlands and Germany. Collaboration took place with other agencies, public-sector bodies and also the private sector. In the main, such collaboration was between banking institutions and the private sector. Interactions with CERTs were also indicated (ENISA, 2010). Outreach activities included public messaging campaigns and information-dissemination efforts (across a variety of media such as radio, TV and the web) and other limited campaigns focused specifically on children, for example.

4.12 Impacts

During interviews we asked respondents to comment on the impact of their unit on cybercrime, their outputs and outcomes.

We anticipated that this would be a difficult question to answer. As described above, the "dark" figure of cybercrime means that data that might be used for performance measurement are lacking. Further, common metrics of criminal justice systems – such as arrests and prosecutions – are not always appropriate in the cyber field where intelligence-gathering and disruption are equally, if not more, valued. As in other areas of crime, these type of metrics measure police/law enforcement resources used rather than the problem itself. Cybercrime is by no means unique in this respect. Even measuring throughputs like number of cases referred, or computers that were forensically analysed is problematic, since cases can vary hugely in their complexity and, as we were told by Spanish interviewees, such metrics "do not necessarily reflect whether the work was done in the right way".

Another potential barrier to assessing impact and effectiveness, mentioned by a Swedish interviewee, is that the unit assists in investigations of crimes that are led by other departments – and it is not always possible to follow the case through to see whether their forensics were used successfully in court.

Despite this, all the units with which we spoke undertook some form of performance-monitoring and made a report of outputs annually, and/or to individuals and oversight committees – for example the Spanish unit provided information to go into a report to the Secretary of State for Security. In Italy, data were sent on a regular basis to the Public Security Department of the Home Office. Italy provided the research team with an indication of the type of data included in these reports (these were set out in Section 2.5).

Interviewees in Ireland said that the unit reports “qualitatively” – in order to reflect the nature and complexity of the work undertaken and the cases in which it has been involved. Similarly, SOCA described how they reported on their disruptive activities in a “narrative” way, and that the quality of intelligence was evaluated through a process similar to “peer review”.

Where there were not available data, we asked interviewees for their personal impressions – based upon their experience and expert judgements. In response, interviewees could point to cases in which the specialist unit had made valuable contributions or in which a criminal network had been disrupted.

4.13 Concluding remarks

This chapter has provided an overview of cybercrime efforts, at the national specialised unit level, across 15 of the EU Member States. From interviews conducted with personnel from these units, we discovered that cybercrime was interpreted in different ways. We found complexity in how the units were structured at the national, regional and local level. We saw that units, in general, conducted activities relating to forensics and investigations but not every unit conducted strategic high level intelligence. We also saw varying degrees of participation in pan European systems such as the AWF Cyborg. Some units we visited reported collaborations with Interpol or other non EU countries and a few had established public-private arrangements with organisations from the financial services sector, for example. We also discovered that provision for training was inconsistent and susceptible to pressing operational demands. We found that with some units, success was not necessarily measured by numbers of arrests.

CHAPTER 5 The role of European-level stakeholders

In this chapter we summarise findings from interviews and supplied documentary evidence from representatives of the four main EU-level organisations – Europol, Eurojust, ENISA and CEPOL. It should be noted that these summaries are a snapshot in time of the period during which evidence was collected (June–September 2011) and therefore since then facts detailed below may well have been superseded by events. Our inputs for this chapter are broader than interviews alone because the current activities and resourcing of these stakeholders has a more direct implication for consideration of the feasibility of an ECC.

5.1 The role of Europol: providing criminal intelligence analysis and operational support to tackle cybercrime

Europol is the pre-eminent organisation in Europe charged with an addressing serious and organised crime at European level. Broadly, it conducts intelligence-gathering and analysis to support law enforcement personnel in the Member States, provides forensic support and co-ordinates a number of other relevant activities.

The legal basis for the establishment of Europol stems from the Europol Council Decision (ECD) of 2001. The establishment of Europol as an EU Agency (taking its funding from the EU budget rather than MS contributions) was agreed just before the entry into force of the Lisbon Treaty (Nov 2009).[24] This placed Europol on a par with other EU agencies such as CEPOL and Eurojust. The implication was that the Europol Council Decision immediately required a recasting to take into account the requirements of the removal of the pillar structure and assumption of new co-decision powers between the European Council and the European Parliament. A new Regulation is expected to be brought into force in 2013. Europol achieved Initial Operating Capability in 2002 with a view to filling intelligence uncertainties in Member State-understanding of cross-border serious and organised crime.

Oversight and strategic governance

The oversight and strategic governance arrangements for Europol are complex, understandably so, given its remit as a pan-European LEA. In the Council, the Standing Committee on Operational Co-operation on Internal Security (COSI) and CATS (the

[24] Proposal for a COUNCIL DECISION establishing the European Police Office COM(2006) 817 final

Article 36 Committee) are the two committees that exercise oversight over Europol. In the European Parliament, the LIBE committee, although not having legal status over the Agency, exercises oversight through determinations on financing decisions.

Within the Agency, the Management Board is made up of representatives from the 27 Member States (coming from the Europol National Units) and a representative from the European Commission. The Management Board meets five times a year. The ENUs are set up according to the particularities of the law enforcement regime in each Member State governing serious and organised crime (e.g. where there is more than one relevant law enforcement authority in the Member State).

There is also a Joint Supervisory Board (JSB) on which all Member States are represented, which includes experts in the specific field of data protection and law enforcement. The JSB is established under Article 34 of the Europol Council Decision and meets five times a year. In addition, there is also a Security Committee made up of experts who exercise oversight over the IT security measures.

Given Europol's operational role, the question of the protection of personal data is taken very seriously. Data Protection at Europol is supervised on various levels and throughout different stages when personal information is being processed by Europol. In particular, Europol's Data Protection Officer must ensure lawfulness and compliance with data protection-related provisions in the Europol Council Decision and implementing rules.

Budget and staffing

Between 2003 and 2008, when Europol was financed directly by Member States, its budget went from €57.8 million to €67.9 million.[25]

According to Europol's final budget and staff establishment for 2011, Europol's budget was nearly €84 million (Europol, 2011b and Europol, 2011c). It employs 457 personnel based at brand-new headquarters (opened in July 2011) in The Hague, Netherlands.

Europol's organisational structure is split into:

- X – Corporate governance/management (including external affairs; legal affairs)
- C – Capabilities (including human resources; IT; finance)
- O – Operations (including terrorism, analysis &; criminal finances and technology)

When we visited Europol in June 2011, it was reported that there were seven Europol personnel currently engaged in addressing cybercrime, within the High-Tech Crime Centre (HTCC), spread across the Operations Directorate.[26] These personnel include individuals conducting intelligence analysis on the Analysis Work Files (AWFs, see below), including those for cybercrime ("Cyborg"). Six personnel work on the child sexual

[25] House of Lords European Committee Report (2008)

[26] It is understood that the period between the collection of this evidence and preparation of this report has seen additional organisational and personnel changes within Europol. However, for reasons of clarity and simplicity, we base our further analysis on the record from our data gathering in June 2011.

exploitation database ("Twins") and others on payment card fraud ("Terminal") in addition to Intellectual Property theft.

Internal planning indicated to us in June 2011 was that there were plans to increase the complement to a maximum of 17 personnel in the future. It is understood that Europol has a plan to undertake consolidation of the many AWFs into just two: one covering organised crime and one covering terrorism based on regional criteria. Nonetheless, despite this consolidation, cybercrime, due it its high degree of technical speciality, was reported as having been afforded the status of a priority area within Europol.

In order to facilitate the work of Europol, all Member States, and even a number of other third party states, have identified personnel as available for interaction with Europol (via Seconded National Experts and Strategic and Co-operation Agreements). The number, quality and spread varies per country, and ranges from larger units to a limited number of specific individuals. This network has been developing over time.

An Operational Centre has been established in "O" Directorate which provides a common interface and helpdesk for incoming SIENA (Secure Information Exchange Network Application, see below) message traffic. This is staffed by 20 personnel on an extended EU working-hours basis (i.e. during working hours across the three time-zones of the EU). This is because it was found that there was no requirement to have a 24/7 capability in this regard.

Activities

Europol's HTCC has three main objectives: firstly, to provide investigative support by co-ordinating and contributing to Member State investigations. This includes operational analysis, specialist forensic support and technical activities. Secondly, Europol's HTCC, by the production and analysis of intelligence, aims to improve knowledge about criminal behaviour. Finally, Europol conducts outreach to a variety of other stakeholders via training and liaison. A number of Europol-wide tools support these activities.

Analysis Work Files

Europol's main tools are the Analysis Work Files (AWFs) – intelligence databases that Member States can submit information to, and request information from.[27] The objective of these databases is to support ongoing 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 line with its EU-level mandate, Europol has criteria that each AWF should be concerned with crimes affecting more than one Member State. Europol analyses the information in these databases in order to identify broader patterns. This analysis is turned around as "product" to Member States and also used to inform Threat Assessments. In late 2010 Europol produced its first iOCTA (Internet-Facilitated Organised Crime Threat Assessment).

[27] According to information provided to the study team, the AWF infrastructure is in the process of being merged into two larger systems – one to address serious and organised crime and one to address terrorism.

AWF Cyborg in particular has a focus on Internet/ICT-driven organised crime, motivated by financial gain. This includes crimes defined within Art 2–8 of the Budapest Cybercrime Convention (including but not limited to identity theft, e-banking scams and e-commerce fraud and e-laundering). Initially, it was reported that AWF Cyborg was focused upon malware-driven e-banking attacks.

AWF records can be linked to forensic data (see below), but they represent meta-information which has a reference to the associated data. It is understood that the process of contributing to and interrogating information from the AWFs is characterised by a three-layer model that is driven by the classification that the originator wishes to apply to the information.

Opening orders are the main means to respect applicable data-protection principles (according to Article 14 of the ECD).

As may be expected, each AWF relies upon the quality of information provided. If Member States see that there is benefit in the information then they might be expected to view participation favourably.

Secure Information Exchange Network Application (SIENA)

In order to allow Member States (in the ENUs) to communicate and share intelligence, SIENA has been established. SIENA is a VPN (Virtual Private Network) based system that allows ENUs to communicate securely with Europol and the AWFs. SIENA is highly regarded by stakeholders as an important tool for the secure and trusted exchange of information. According to Europol's own figures, on average, 25,000 messages have been transmitted over SIENA each month since its launch in 2009. SIENA is security accredited up to the level of EU RESTRICTED and allows for upgrade to further classification levels. Handling of information is possible up to the highest level, EU TOP SECRET. SIENA was developed with Privacy by Design principles in mind concerning the fulfilment of data-protection and security requirements.

IFOREX – Internet Forensic Expertise

IFOREX (Internet and Forensic Expert Forum) is another set of activities performed by Europol concerning the exchange of forensic best practices. This is aimed at building a knowledge-base of guidance on technology-related matters concerning best practices and training on forensics. A repository of scripts and software has been established and IFOREX users are encouraged to contribute best practices and share information. Support is also offered to Member States in their investigations (see below).

Computer Forensic Network

A major development at Europol is the investment in a new Computer Forensic Network (CFN). The CFN is an IT resource that operates within Europol (but not over SIENA) and is a dedicated network for computer forensics. CFN supports the extraction of a legal technical copy of the data and sits alongside the AWF environment – acting as a repository for pre-processing. It is a horizontal system, in that it supports intelligence and operational activities across all types of crime commodities (not just cybercrime). Data is recycled after usage so the storage capacity is a product of the number and length of investigations not the necessarily quantity of data.

The example of "Operation Rescue" is instructive in this regard, highlighting the forensic capabilities required. Combined between the UK, Netherlands and Australia, IT support was required to recreate the data (discussion forum concerning child exploitation) – there were 700 suspects, 4TB of data, 200 suspects arrested and 230 children identified.

CFN operates in effect across three levels of complexity of forensics:

- At the first level, CFN is usable by all units – it is an accredited platform and it is audited as AWF. Its benefits are making the legal technical copy more accessible, it can be used for different sorts of file storage system (e.g. FAT32, Linux, mobile, GPS) and it provides greater security and protection against viruses.
- At the second level, with regard to the AWFs (Twins, Cyborg, forgery of money, etc.) it allows more forensic-orientated analysis.
- At the third level, it is dedicated to HTCC: it allows the exploration and conduct of research and development activities to support the fight against cybercrime. These tasks might include, for example, decryption and the exploration and forensic analysis of malware. With respect to the latter it is hoped that the R&D lab will be ISO accredited shortly.

Currently there is 500TB storage space and further expansion is expected in 2012.

There is also mobile digital forensic support capability, to support the principle of chain of custody in deployed environments and also to act as a flexible resource for Member States, which can be deployed at the invitation of Member States. This takes the form of a mobile office and other tools that the MS request support with (e.g. mobile 'phone forensic capabilities).

The mobile office connects to Europol in real-time via a live link, allowing searching of AWFs and the CFN and secure interaction with other Europol systems. The mobile office can only work within the legal framework of the Member State (e.g. in respect of personal data processing) that is to say it is governed by the same regulatory framework as the ENUs with respect to what is and is not permissible.

ICROS – Internet Crime Reporting Online System

The ICROS is an initiative to facilitate the online reporting of all offences noted on the Internet and reported at domestic level. It is reported to be at the requirements-gathering phase in Europol and has received some funding from the European Commission. The objective of ICROS is that by collating online reporting systems, greater understanding of emergent pan-European threats may be achieved via a centralised repository of crimes. This would allow the further development of preventative strategies and help MS in understanding where to steer their crime-fighting strategies going forward. At present it is uncertain whether ICROS will be a standalone system, integrated via backend "interoperability" with existing Member State reporting systems or whether it will be a meta-resource or portal redirecting visitors to the appropriate national mechanism.

According to the ICROS status report of late 2011 (Europol, 2011d), a number of functions have been identified that are regarded by Europol as key, including: reliability, sharing and exchange of operational data, a comprehensive and reliable overview of Internet-related crimes, input to analytical activities, statistical data-generation and the processing and exchange of information. In 2012 it is understood that deliverables for ICROS will revolve around the online facilitation of Internet crime reporting, an expert platform open to both public and private partners, a restricted environment for the centralised storage and processing of operational data and finally facilitation of automated data exchange. In 2011 it was understood that a technology discovery phase was underway to identify the most suitable solution given Europol's unique regime concerning personal data protection and its legal basis.

EIS and EPE

Europol Information System (EIS) and EPE (the Europol Platform for Experts) are two other information systems that facilitate the work of Europol. They have been established with the involvement of the Joint Supervisory Body and with respect for data protection principles. EPE is envisaged by Europol as a common solution for communication needs of expert communities operating within Europol's mandated areas (i.e. not just within cybercrime).

Training

In addition, Europol has links to ECTEG (currently chaired by the Irish Garda High-Tech Crime unit). ECTEG has 40–60 members as permanent participants and involves LEAs, international organisations, private industry and universities. It also works on harmonisation of training for cybercrime and has provided input into a university-accredited syllabus (under the remit of the Bologna Convention concerning mutual recognition of qualifications). UCD runs an MSc in Forensic Computing and Cybercrime Investigation. ECTEG also conducts continuous follow-up in development and delivery of training modules.

Examples of the subject of different training courses include introductions to IT forensics and investigation, conducting forensics across different platforms (NTFS, Linux, mobile 'phones) Internet and network investigations, malware analysis and live data forensics.

5.2 Eurojust – supporting judicial co-operation in cybercrime investigations

Eurojust was established in its current form in 2002 by the Framework Decision on Eurojust. It works to dismantle transnational organised crime networks by facilitating co-ordination and providing advice on legal and regulatory frameworks issues of jurisdiction.

Eurojust works to improve co-operation between the judiciary (i.e. prosecutors and judges) and via its links with Europol, the broader criminal justice community. In this way it might be seen as an important partner to Europol in respect of those aspects of law enforcement work relating to policing and the effective operation of the criminal justice system.

Eurojust also gives opinions and advice – both on substantive law and relevant policy development – to other European institutions.

Budget and staffing

Eurojust's budget was €32 million in 2010–11 and €34 million in 2011–12. Eurojust has 308 personnel based in The Hague. Eurojust staff are employed and empowered by their home country (not European employees). The powers of a national member depend upon the implementation of the Eurojust decision by their home country.

An operational, problem-solving role

Interviewees from Eurojust highlighted their operational role. They provide support to prosecutors in Member States in cases that Member States chose to refer to them (there is no obligation for a Member State to refer a case to Eurojust)[28]. In this role, we were told that it is important that the Eurojust national members are "insiders" from the country, rather than a European, external influence.

Eurojust operates an on-call reporting function called "Encore", which prosecutors in a Member State can call to report cases and offences at any time and get immediate support and advice from Eurojust.

Eurojust also facilitates the establishment of Joint Investigation Teams (JITs), which are set up to respond to particular cases and are intended to speed up the process of requesting information. Interviewees commented that JITs are especially important in cybercrime because the success of the investigation depends a lot on speed. As part of a JIT, Eurojust can set up a co-ordination centre (perhaps only convened for one day) to pool and share data as quickly and efficiently as possible as an investigation is being carried out.

Collaborations

Interviewees described Eurojust as "complementing" Europol, and described several forms of co-operation – including JITs and delivering training. Eurojust participates in training facilited by CEPOL. Europol is starting some informal co-operation with ENISA and cooperation with the private sector was described as "developing".

Cybercrime at Eurojust

Eurojust has a Financial and Economic Crimes Team, and dealing with cybercrime falls within this. However, it is clear from the interview that when referring to "cybercrime" interviewees were taking a broader definition than just the Budapest Convention. They stressed that there is often a "cyber" element to many types of offences – rather than the term representing a discrete crime type – that can blur into terrorism, online child

[28] We were told, however that there is now a duty on Member States to report certain serious offences to Eurojust. This data can help Eurojust have better information and offer support and advice in cases.

exploitation, and so on. Following from this, dealing with cybercrime cases demands a range of different skills depending on the nature of the case.

Twelve people work in this Financial and Economic Crime Team, drawn from different national desks and areas of Eurojust (magistrates, prosecutors, etc.). Three or four people particularly focus on cybercrime, although the understanding from the interviews is that no one seemed completely to specialise in cyber, and that cyber issues are dealt with by people from different teams. Interviewees reported that there is an expert analyst working in the cyber field at Eurojust (an ex-Europol employee) who provides operational and strategic-level support.

Some of the activities undertaken by the unit, in additional to operational support to Member States, included "strategic calls workshop" in which specialists discuss the evolution of laws and regulations to try to stay aware of the evolution of the cybercrime environment, and a "Strategic Seminar" held in Greece in 2008. This was aimed at Member State judges and prosecutors where participants shared best practice and discussed cases and tools that judges and prosecutors could use.

Barriers and facilitators in relation to cybercrime

During the interview with Eurojust members, the following issues were raised.

Training

Interviewees reported a gap in training within the EU and the existence of significant differences in knowledge between judges and prosecutors in different countries. We were told that judges and prosecutors want to deal with cybercrime, but lack the necessary training (which risks that the defence is better-equipped than prosecutors).

Some examples of good training programmes were cited, for example the French École nationale de la magistrature (National School for the Judiciary) provides specialist training for judges and prosecutors in cybercrime. Interviewees also mentioned that some prosecutors had taken part in law enforcement training.

Legislation in MS

The variance in legislative frameworks in the Member States is a challenge. Even if a country has ratified the Cybercrime Convention, they might have done this inconsistently and different Member States still have provisions. In addition to Convention, Member States have their own, separate laws. In response to this, interviewees suggested that common minimum standards would be helpful. However, in addition to the criminalisation of particular cyber activities, an issue which can be as, if not more, troublesome is the lack of common evidential standards. Evidence rules and standards are very important but are not covered in detail in the convention.

Third countries

Interviewees noted both the importance of, and the difficulties in contact with, third countries. We were told that Eurojust has a formal co-operation agreement with the USA and some other third countries, but there are limits to the ability of Eurojust in securing co-operation.

Technicality

Cyber cases are complicated and technical. Interviewees gave an example of a case involving hacking into the French Ministry of Justice where national prosecutors and judges needed to be able to quickly access advice and a lay description of what had happened.

5.3 European Network and Information Security Agency – facilitating co-operation and best practice on cyber-security

ENISA was set up in 2004 to "ensure a high and effective level of network and information security (NIS) within the European Community (Union) and to develop a culture of network and information security within the Community." ENISA has 62 personnel based at its headquarters in the island of Crete. ENISA staff can undertake missions to locations across Europe (and further afield). ENISA also provides a Mobile Assistance Team to serve the Member States. We were told that there are three members of staff at ENISA who work in, but are not uniquely dedicated to, cybercrime. ENISA has established a role for itself as a trusted intermediary to the European Computer Emergency Response Team (CERT) community.

ENISA's annual budget is approximately €8 million. The one activity that ENISA is currently undertaking in relation to cybercrime (WP2011/WS1/WPK1.5) has been assigned €120,000 in 2011.

ENISA's role, improving network and information security across Europe, clearly has an interface with preventing cybercrime. Secure networks and secure information are a strong defence against cybercrime, and an understanding of security issues can assist with detection of crimes when they occur.

Cybercrime is not specifically within ENISA's remit and it has no legal powers in relation to operationally addressing cybercrime. However, there are many areas in which ENISAs activities in ensuring network and information security overlap with the response to cybercrime in Europe, and these overlaps have been explicitly noted in official strategies and documents published by ENISA and the Commission.

The EU's Internal Security Strategy makes a number of references to how ENISA can support the Member States in the fight against cybercrime by raising levels of security for citizens and businesses using cyberspace. The following activities for ENISA are explicitly identified:

- Co-operation with the European Cybercrime Centre.
- Contribution to the development of a European Information Sharing and Alerting System (EISAS) for the general public before the end of 2013.
- Support for the Member States in the elaboration of national contingency plans.
- Assistance to the Member States in organising regular national and European exercises in incident response and disaster recovery.

A major element of ENISA's work is the support it provides to CERTs, and ENISA's Work Programme for 2011 includes an activity called "Good practice for CERTs to address NIS aspects of cybercrime" which is likely to be continued in 2012. This activity aims to improve CERTs' capability in addressing NIS aspects of cybercrime. The outputs from this work will be a good practice guide for CERTs in addressing NIS aspects of cybercrime and ENISA's sixth workshop for CERTs in Europe.

Links with stakeholders

ENISA has strong links with the public *and* private sectors. ENISA interacts with the private sector in the field of cybercrime through expert working groups dealing with NIS aspects of cybercrime. ENISA describes itself as having "well established relationships with relevant stakeholders both from the public and the private sectors".

ENISA has been active in helping to develop the concept of national/governmental CERTs and supports the CERT community in a variety of ways. ENISA could play a role in bringing together organisations working in NIS, such as CERTs, with organisations directly working in cybercrime, to share good practice and establish dialogues.

ENISA has embarked upon facilitation activities to reinforce co-operation between national/governmental CERTs. These activities (such as workshops, exchange of best practice and training) include measures to improve co-operation at national level between national / governmental CERTs and LEAs.

ENISA's relationships with Member States in relation to cybercrime are mainly through the Management Board (MB) and National Liaison Officer (NLO) networks, and through events co-organised with the Member States. We were told by ENISA that cybercrime is sometimes a main theme at these events, but "is a constant element in the discussion of network and information security".

Developing relationship with other institutions

ENISA participates in conferences, meetings and other events on cybercrime, with, for example, the Council of Europe, Europol and CEPOL. In 2011, a delegation from Interpol visited ENISA and synergies among the two institutions were explored. In 2011 ENISA participated in the European Union Cybercrime Task Force (EUCTF) meeting, and also took part in Interpol's first cybercrime training workshop.

ENISA is currently developing a Memorandum of Understanding with Europol. This is intended to "enable the two agencies to exchange certain information relating to cybersecurity in a structured way". No further information was available as to what type of information might be exchanged.

5.4 CEPOL – strengthening capability with training and professional development

The European Police College has 42 officers based at Bramshill in the UK. CEPOL's annual budget was around €8.2 million in 2010–11. CEPOL's training activities are aimed at senior and middle-ranking law enforcement officers across Europe. It also co-ordinates capacity-building activities in third countries such as Mexico, Afghanistan and Iraq by co-ordinating police missions.

The CEPOL model

CEPOL training programmes are delivered and implemented within and by the Member States and organisations that are CEPOL's partners – there are over 40 partners across the EU – at least one in each Member State, including police colleges and universities. CEPOL offers grants to cover travel costs of those who attend training courses, but it does not fund or deliver those courses. It is part of the CEPOL model that the skills and expertise to deliver training come from the network of partners, facilitated by CEPOL. CEPOL sends an observer to training programmes paid for by CEPOL grants.

The interviewee perceived that one of the ways in which CEOPL adds value is through allowing law enforcement practitioners from different countries to meet each other and develop networks. Such bilateral relationships can be important in dealing with cyber cases.

Collaborations

The interviewee said that CEPOL collaborates closely with Europol. It is part of CEPOL's remit to spread knowledge about Europol, and training courses are quality assured and co-designed by Europol. CEPOL arranges study visits to Europol. Similarly, good co-operation was reported with Eurojust, with which CEPOL has a co-operation agreement. CEPOL has developed joint training on JITs with the European Judicial Training Network (EJTN). Currently, there is no formal co-operation with ENISA, in part because the overlap in the area of cyber is only a small part of CEPOL's work.

There are plans for CEPOL gradually to assume functions and tasks currently carried out informally by ECTEG. CEPOL and ECTEG currently have an informal relationship in which they co-operate to develop the training packages currently offered by ECTEG with support from UCD.

Private-sector experts are involved in CEPOL's programmes, but are not official partners. In respect of third countries, the interviewee suggested that co-operation on training with countries such as Russia is less contentious than operational co-operation. We were told that CEPOL has received requests for joint training and collaboration from countries including the USA and Mexico.

Cyber activities at Europol

Similarly to interviewees from Eurojust, CEPOL representatives stressed that cybercrime is a cross-cutting area. We were told that CEPOL currently holds about 10 activities specifically about cybercrime, in which 236 people have participated. Whilst there is no assigned expert on cybercrime within CEPOL's 42 staff, that is not unusual, and is in keeping with CEPOL's model of operation, which is to second experts and bring in people to offer advice. There is currently no common curriculum across MS on cybercrime. In seeking to improve cyber-related skills, there is a challenge in starting from very different baselines in different countries.

Some activities explicitly relating to cyber include:

E-learning module on cybercrime

This is aimed at high-ranking police officers. Europol, ECTEG and the Member States have all been involved in its development. It will include pages on:

- Co-operation (EU/international/private sector/universities/different police forces and departments within a MS)
- Institution building
- Prevention
- Legal frameworks
- Cases – including case management
- First response – including dealing with Internet evidence
- Investigation – evidence-gathering and intelligence-gathering
- Digital forensics
- Network forensics
- Presentation (evidence admissibility).

Exchange for cyber experts

CEPOL has operated an exchange programme for several years, but in 2011 launched a strand of this specially for experts in national cybercrime centres. Under this programme national cybercrime specialists will spend time in a unit in another country. We were told that interest in this programme has been expressed by countries outside of the EU.

Webinars

CEPOL operates several "webinars" (online seminars which are accessible to a broad audience) on cyber-related topics. For example, CEPOL staff developed a webinar on IPv6 at the end of 2011, and we were told that experts from ENISA were involved in its design.

Mapping skills and training needs

This activity is not only related to cybercrime, but will cover cyber skills. A European Training Scheme for law enforcement has been established by the Commission, and as part of this the Commission has asked CEPOL to:

- Map existing law enforcement in Europe: customs/border/police forces, etc.
- Map existing international training (including bilateral agreements)
- Undertake a gap analysis
- Identify training needs for the next five years

This information will be collected via a questionnaire that Member States will be asked to complete. The mapping should be completed and available in February 2012.

5.5 Conclusions

As can be seen from the discussions in this chapter, there are many different activities that are undertaken and developed by different stakeholders in respect of addressing cybercrime at the pan-European level. Each of these must come together in an efficient and effective way in order to have any impact on the phenomena of cybercrime. However, the different resources, risks, legal basis and institutional characters of each of these organisations may present challenges with respect to working collaboratively going forward. In particular, establishing how the different motivations between the private sector and law enforcement and criminal intelligence community may be satisfactorily addressed, whilst respecting fundamental human rights, will be of paramount importance for the future, as well as keeping up-to-date with how the threat and *modus operandi* are evolving and new opportunities for information technology and cyberspace to be exploited by criminals.

PART III

CHAPTER 6 Developing options for a European Cybercrime Centre

6.1 Options analysis

In this chapter of the report, we present an emergent range of draft options or "models" for the ECC. This is based on two main sources of material: evidence derived from our empirical fieldwork (interviews with the key EU institutions, 15 Member States and industry) and the results of our collective discussions of the evidence at an internal evidence review workshop held by the study team on 20 September 2011. This was supplemented by findings from the literature review. The objective of the internal evidence review meeting was to:

- Develop a clear linkage between the evidence derived from our fieldwork trips and what gaps or objectives an ECC could support or address, as determined by collected data from the data sources (and noting the open question about whether the ECC should be there to merely fill gaps or provide some additional added value).
- Establish the areas of divergence/coherence between the desired or required objectives or requirements for an ECC from our interpretation of the evidence and that which has already been envisaged in the policy-making process (e.g. the 2010 Internal Security Strategy).

At this meeting, we identified a range of objectives that the evidence (and our collective interpretation of it) suggested an ECC could accomplish, via a range of measures. In addition to these objectives, there seemed to be an emphasis from the fieldwork on the global nature of cybercrime (often requiring interaction with third countries outside of the EU and other globally relevant law enforcement organisations such as Interpol) and the need to create a culture of trust between the different perspectives (enabling the exchange of information) particularly pertinent with the public–private sector linkages.

6.2 Tasks envisaged in the policy discussions so far include:

Our starting point for the options development was to draw up a list of activities which an ECC could or should undertake. These are set out below. The list consists of:

- Activities that are currently undertaken by National High-Tech Crime Units. These were described to the research team during interviews and are set out in

Section 4.5. An ECC may wish to support these activities in order to add value to Member States' Law Enforcement Authorities.

- Activities that Member State-level interviewees explicitly identified as activities for any future ECC.
- Activities that the research team identified to address issues which Member State-level interviewees highlighted as being current barriers to dealing with cybercrime.

In addition, we have in mind the objectives for an ECC set out in the Study terms of reference as noted in Chapter 1 of this report.

Each of these possible activities could be executed in different ways – via an operational, collaborative or advisory approach (in decreasing order of depth of intervention).

- Providing investigative support
    - Help in facilitating Mutual Legal Assistance Treaties
    - Facilitating the set-up and running of JITs with cybercrime components
    - Providing specific investigations support (direct support e.g. via forensic capabilities).
- Gathering intelligence (incentivising contribution to information exchange and analysis linking to other crimes), specifically on:
    - Intelligence databases (info exchange)
    - Hotline and public reporting input (awareness)
    - Trend monitoring (awareness)
    - Defining intelligence requirements.
- Conducting outreach (to the broad range of stakeholders such as the private sector, industry, citizens, etc.) concretising the link/input of the private sector
- Developing contacts and networks (seen as crucial enabler of trust, e.g. for police working together)
- Providing strategic advice to policy-makers
    - For example, in articulating the implication of specific legislative frameworks or providing perspectives in debates on the harmonisation of legislation.
    - Acting as the collective "voice" of High-Tech Crime Units across Europe (i.e. placing the EUCTF on a firmer footing).
- Supporting a hotline or one-stop shop (n.b. this is not a reporting hotline but rather a facility for investigators or law enforcement/criminal justice professionals to request support, advice, etc.)
    - For prosecutors
    - And for non-specialist forces.

- Delivering/conducting training and good practice sharing
    - For forensics teams
    - For prosecutors
    - On the use of tools (e.g. how to image a particular device)
    - On IT literacy (facilitating the training in general areas such as "How does IPv6 work?", or "What are the implications of cloud computing, for my role?")

6.3 The Draft options

Below we set out some options. In creating this list we applied the guiding principles that there needed to be a small enough range of options to make the list manageable, but keep it broad enough to allow the participants in the next stage of research to consider different and innovative ways of addressing the problem, based on the range of possible types of intervention.

This list developed from our matching an estimation of what would be broadly possible (not necessarily a strength or a weakness) in terms of the types of intervention as described above given the current activities and role of the stakeholders.

Other high-level issues arising from the analysis of the current situation would seem to indicate that the complexity of intervening directly in local regimes and structures would be prohibitive. The countries included in our research exhibited variable and highly different regional and local politico-administrative arrangements that were driven by a range of historical, cultural and legal factors. Therefore it would appear to make sense that the ECC would operate only with the national-level units as its constituents rather than the *entirety* of the cybercrime police in each Member State.

6.4 Draft option 0: Maintain the status quo

This option involves improvements of current activities of the stakeholders identified in the research so far. For example, in this option we would envisage measures to strengthen the use of the intelligence databases by Member States, identify ways in which the combined voice of the heads of national HTCUs could be heard (e.g. through the EUCTF) and further strengthen existing activities and capabilities (e.g. with respect to training provision).

The next group of options we look at below concerns the feasibility of modifying existing relevant structures.

6.5 Draft option 1: An ECC owned by Europol

This option has a lot of favour and interest at present, given Europol's role and current remit, especially the operational nature of the organisation. Provision of investigative support (forensics, support with other MLATs and Joint Investigation Teams) would be of an operational or collaborative nature given Europol's current mobile forensic capabilities, network and also links to Eurojust. 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 (albeit with room for improvements). With regards to outreach, this would be envisaged as collaborative in nature given the current legal framework as to what can and cannot be shared with the private sector (and also the emergent state of relations within 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 the national HTCUs and other partners (e.g. industry). Running an internal "one-stop shop" hotline could be an operational activity (in the same way as the current intelligence databases). Finally, if Europol were to try to achieve the objective of training then it would have to be a collaborative exercise, working alongside other training partners (such as CEPOL, ECTEG, academia and industry), noting that Europol also provides some training (e.g. in investigative techniques).

6.6 Draft option 2: An ECC owned by Eurojust

As the other operational agency, many of these aspects described above with respect to Europol are also relevant to Eurojust. Eurojust already operates MLAT support functions and JITs so achieving this objective would have an operational nature. However, providing intelligence functions would have to be collaborative since Eurojust would need to either rely 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, because this would require the collation of views from Member States (and also an agency with a judicial remit might be legally unable to represent the views of an operational police community). 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 it does now. Finally, if Eurojust were to try to achieve the required objectives indicated from our fieldwork of addressing training provision, then 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 it currently does not carry out any training activities.

6.7 Draft option 3: An ECC owned by ENISA

As 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 type of activity rather than direct operational intervention. ENISA has neither operational responsibilities nor mandate in the field of cybercrime. It would be highly unfeasible for ENISA to undertake direct investigative support nor intelligence sharing since these are tasks that the Agency currently does not do and has no competence nor mandate. It would also be highly infeasible to adapt ENISA's mandate to this end since the option of changing the legal basis to possibly accommodate ENISA's mandate is not considered in the current legislative process (revision of the Regulation concerning ENISA) engaged in Council and European Parliament. Outreach could be performed more collaboratively, since, relatively speaking, ENISA already has better links with many of the non-law enforcement stakeholders (especially private industry) than the other current EU level stakeholders. The one area in which ENISA could take an operational role is in delivering training (since the Agency has already delivered exercises and also delivering training for LEAs and CERTs). Given that the option of ENISA hosting the ECC is currently not doable, there is clearly no need to explore it further.

6.8 Draft option 4: an ECC as a virtual centre ("exchange", "switching centre"; "clearing house")

A final option in this group would be to create a virtual centre, which would nonetheless require some modification to the existing structures and might have additional administrative and bureaucratic implications (in establishing frameworks for interoperability between the existing stakeholders). The virtual centre would leverage existing capabilities in each relevant stakeholder (for example, Europol with its intelligence capabilities, provision of investigative support, etc.) in an advisory capacity (directing queries to other, better placed stakeholders). The challenge in this model would lie in establishing strong overall guidance, so some form of collective board or decision-making authority would be required to ensure that each stakeholder is incited to accept responsibilities, contributes fairly and works collectively and collaboratively, reaching back to capabilities within their respective organisations to address problems jointly. This would suggest that an independent non-partisan but expert chair would be required to marshal the efforts of these organisations.

The second group of options we can characterise revolves around the establishment of a wholly new structure on a "clean sheet" basis. This could take the form of a new EU-level agency or body, an agency or body run within a Member State or an EU-level Public–Private Partnership.

6.9 Draft option 5: A new EU agency

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 from the fieldwork. For example, addressing the objective of supporting Member State investigations of cybercrime would be done in a collaborative or advisory nature, 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 intelligence capabilities of Member States. The remainder of the tasks could be undertaken on an operational basis since the mandate of a unit (being from a blank sheet of paper) could be designed specifically around implementing measures to address these objectives. For example, the "on call" facility of Eurojust could be instead 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).

6.10 Draft option 6: One Member State running an ECC on behalf of the Union ("SIS II Model")

In this draft option a single Member State would be responsible for the operational running of a new agency, on behalf of the Union. The precedent for this is the management agency for the second generation Schengen Information System (SIS), which is run by the French government (and staffed by French law enforcement officials) on behalf of the rest of the Union. In this option, the specific legal, contextual and administrative structures might mean that 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. This option might be more suited to an ECC which has a clearly defined technical role – for example, specifically for the running of an online reporting platform.

6.11 Draft option 7: Public–Private Partnership (PPP)

In this final draft option, a joint 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 co-ordination) 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) in order to meet some of the requirements identified from the fieldwork. 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 from a PPP could support such interaction.

6.12 Conclusions

This chapter has indicated how we identified a broad range of possible options stemming from maintaining the status quo to a wholly new agency. In the next chapter, we focus on four specific options for further consideration, noting that the options that might bring the ECC into being should be driven by consideration of a broad pan-European-level capability to address cybercrime, which involves the many organisations from both the public and private sectors that have a role to play.

CHAPTER 7 Analysis of the four candidate options

7.1 Introduction

The previous chapter discussed how we arrived at a list of eight draft options for consideration. This list of eight was elaborated as a way to engage participants in further options workshops to consider a wide range of possible considerations about how the ECC could be established.

In the next phase of our research, we identified four options out of the eight outlined in Chapter 6 for further detailed consideration. We identified these through two mechanisms. Firstly, we conducted workshops with each of the four main EU-level institutions (see Chapter 5) likely to play a significant role in the ECC. Secondly, the views of these four main institutions were supplemented by input received from Member States and others at a scenario-based workshop in Brussels in November 2011. These workshops suggested that those options which should be identified for further investigation should concentrate upon those which could be rapidly implemented within existing structures, should include Europol in some way and should encourage greater coherence between the different activities which all mesh together to provide an overall capability to address cybercrime.

Additionally, using documents provided to us throughout the course of the study, we extrapolated the Impacts and Resources required for the ECC under these four different options.

Below we compare and contrast the characteristics of each option across the six areas identified as being relevant to the feasibility of the ECC, namely:

- Mandate – what forms of cybercrime should be in and out of scope for the ECC to tackle.
- Activities – what sets of activities or tasks should the ECC undertake.
- Resources – what resources in terms of people or infrastructure are required to perform these activities under two different projected workload requirements. The first represents a broad increase in half as many additional personnel to conduct criminal intelligence and operational support duties (the "low workload requirement") and the second roughly a six-fold increase from the existing

criminal intelligence and operational support personnel (the “high” workload requirement);

- Risks – what are the risks to the establishment and operation of an ECC.
- Co-operation – on what, to what degree, and how co-operation should be established between the main organisations having a role in dealing with cybercrime at the European level.
- Impacts – what sort of impacts the ECC should aim to have.

Notwithstanding the option of maintaining the status quo, we assume that each option would conduct largely the same activities, would work toward the same type of impacts and be exposed to the same risks. However, the degree of strength each option would have in managing these factors, for example, would differ. Thus, for risks, co-operation and impacts we present more of a binary comparison between maintaining the status quo and establishing the ECC (regardless of how it is implemented).

7.1.1 Background

Much is being asked of the ECC in terms of the sheer breadth of activities that it must achieve. The Internal Security Strategy (ISS) in 2010 indicated that the aims of the ECC were to:

- Improve evaluation and monitoring of existing preventative and investigative measures (undoubtedly a significant undertaking, as we have seen from Chapters 2 and 3).
- Support the development of training for the criminal justice community across the Member States.
- Establish co-operation between all stakeholders involved in addressing cybercrime (and the private sector).

These aims are spread across the traditional law enforcement and criminal justice spectrum of criminal intelligence gathering, trend analysis but also supporting and strengthening investigations conducted by the Member States. In addition, a range of tasks including providing for training (of both the law enforcement community and the judiciary), establishing and improving co-operation with the private sector such as CSPs and financial institutions but also other relevant stakeholders (e.g. national/governmental CERTs) and non-EU countries has also been noted.

Another high-profile set of activities revolves around the ECC hosting a reporting platform for cybercrimes. This platform is intended to underpin the reporting and exchange of cybercrime data between a number of different types of entity, including:

- Members of the public to law enforcement

- Businesses to law enforcement
- Law enforcement to law enforcement.

Although the Internet Crime Reporting Online System (ICROS) project run by Europol has made progress in this area, the question of what form such a reporting centre should take – centralised (replacing Member State platforms) or as a separate entity – has still to be resolved.

From the Member State perspective, the fieldwork and subsequent analysis of gathered material suggested that the ECC could help in achieving valuable other objectives such as: providing a platform for the collective voice of cybercrime law enforcement; facilitating internal support via an on-call facility; building and maintaining contact networks; and finally, acting as a broker for the exchange of good practice.

7.2 What outcomes or impacts should the ECC aim to achieve?

Evidence from this study and elsewhere indicates two different approaches to addressing cybercrime {Wall, 2007 #120}. One approach is to find, prosecute and bring to justice as many cybercriminals as possible – a classical criminal justice approach. Another is to engage in preventative activities in order to reduce the opportunity for cybercrimes to take place, disrupt and dismantle criminal networks to reduce harm to citizens. These contrasting though not wholly exclusive approaches, also exist in other criminal justice domains and are not unique to cybercrime. The latter approach is being taken in some Member States due to the recognition that measuring the impact of prosecutions in improving overall levels of security is difficult (due to the unknown nature of the phenomena).

These two approaches are reflected in descriptions of what the ECC should accomplish in the ISS: in Action 1 "Build capacity in law enforcement and the judiciary" and under the heading of Objective 3: "Raise levels of security for citizens and businesses in cyberspace".

These two different approaches are distinct but (could be) mutually supportive objectives (for example, by conducting extensive analysis of cases it may be possible to analyse and determine where the most cost-effective opportunities exist to reduce impacts on society. Nonetheless the implications of setting up the ECC primarily to address one or the other type of outcome are important, since this will inform what legal basis is required, the character of the hosting organisation, the relative focus of the ECC on different activities, the type of personnel employed and the nature and extent of training delivered.

The ISS indicated that the primary objective for the ECC is to support and strengthen investigations {European Commission, 2010 #121}.. The implications of this are that the ECC would need strong capabilities and a legal framework – a governing legal basis – to permit the exchange of personal data (on suspects and victims) to support the chain of evidence for investigations and trial. This is because an explicit focus on investigations requires a different standard of evidence than that used for intelligence-gathering.

Furthermore, the trusted community able to share information when it is at the intelligence stage is a superset of that allowed to handle information as evidence once it becomes part of an investigation.

Coupled with this, it might be that an ECC with a stronger focus on prosecution would need to have closer links with the judiciary – for example, through awareness-raising or training.

The aforementioned activities concerning co-operation and outreach might also take on a different emphasis depending on the focus of an ECC. Developing information-exchange links with the national/governmental CERT and cybersecurity community, and an emphasis on the establishment of a public reporting point contribute more to a high-level intelligence-led approach.

This is reflected in the Council Conclusions of November 2008 on a Council Conclusions on a Concerted Work Strategy and Practical Measures Against Cybercrime[29] which noted the role of the ECC in the collection of statistics on cybercrime. A strategy informed by a focus on these criminal justice outcomes would mean that an ECC could have a more "open" legal regime making interfaces with the private sector less complex, but also requiring a different skill-set of staff.

7.3 Summary of options under detailed consideration

7.3.1 Maintaining the status quo

In this option, no ECC is established and activities continue as they are with the various EU institutions currently addressing cybercrime. It is expected that efforts would continue towards integration of the High-Tech Crime Centre (HTCC)[30] 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 as described in our fieldwork with Europol. Eurojust also continues with its support to the judiciary and public prosecutors and work with Europol on JITs. Furthermore, training efforts continue in the current manner with CEPOL and ECTEG both delivering different types of training aimed at different customers. Finally, ENISA's CERT co-ordination programme develops and refines its interpretation of how to establish co-operation with the CERT community, building upon the first CERT–LEA workshop, held in October 2011.

[29] JHA Council Conclusions 2987th JHA meeting (2008)

[30] As of 20 December 2011 this has been renamed the Europol Cybercrime Centre but to avoid confusion we refer to it as the HTCC

7.3.2 An ECC owned by Europol

There is a clear attraction to the option of an ECC being run at Europol. Europol, as the EU's only criminal intelligence agency, has a clear mandate in this domain and is a well recognised "brand" amongst 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 those 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 role – it has an extensive data-protection regime and a complex set of rules governing participation in the AWFs. This legal basis is due to be revised in 2012 when it is expected that a regulation will be developed. 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 would receive additional resources in order to set up and run the ECC in addition to its existing appropriation. These resources would be concerned mainly with staffing, since extensive physical and ICT infrastructure (as described above) is already in existence.

Europol has supported training and awareness-raising activities via its role on the Board of ECTEG and via delivering specific training courses through its IFOREX platform. More latterly, Europol hosts biannual meetings of the EUCTF (European Cybercrime Task Force) – a platform of heads of HTCUs across the EU, which acts as a strategic voice of the law enforcement community on cybercrime-related issues. Europol has also signed different types of co-operation agreements between third countries (permitting the exchange of personal data) and institutions (e.g. Interpol). Nonetheless, as indicated above, the intelligence and investigative organisational character of Europol could create barriers to the deeper co-operation with other stakeholders understood as necessary to achieve the broader strategic goal of a bigger picture concerning the extent of cybercrime. The training provision currently undertaken by ECTEG is focused on law enforcement professionals and may be not a good fit for use by the judiciary. Participants in this study from Eurojust reported that in their view, public prosecutors and judges do not require academically accredited training.

Furthermore, the necessarily complex governance arrangements of Europol (specifically with respect to the role of the European Parliament and Council) might create additional bureaucracy though when an ECC, hosted in the agency, would try to interact with the private sector. This latter point is particularly pertinent. Currently, Article 25 of the Europol Council Decision acts as something of a barrier for the agency to interact with the private sector.

7.3.3 An ECC hosted at but not owned by Europol

A variation of the option above is an ECC hosted by but not owned by Europol. Under this option, the existing facilities, infrastructure and "brand name" are leveraged by the ECC. However, the ECC would have separate legal personality, budget and an explicit mandate to cover specific types of cybercrime which may be different from that currently defined in Europol's governing legal instrument. In relation to the sorts of activities such an ECC might be able to conduct, these would be as above (in Section 7.3.2). Additional oversight would be necessary, bringing in the perspectives from the other organisations (e.g. Eurojust, ENISA, CEPOL) described above. This oversight might be a necessity if the ECC were to process sensitive personal data (also known as nominal data) in the criminal intelligence aspect of activities supporting Member State level investigations. This oversight would also need to extend to governance of the ECC to act as a natural counterbalance to any possible institutional inertia and to help ensure that the ECC was delivering according to its mandate.

Such an option would be administratively high risk due to the "agency within an agency" character of the option. For example, there would have to be separate operational agreements established (as Europol now has with other organisations such as Interpol) to allow personal data to flow between the AWF infrastructure and the strategic intelligence activities of the ECC. Risks would include those of visibility and the perception of organisational clarity of the ECC in 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. Our research and other work suggests that the private sector has greater insight into real-time incident data and early warning of when incidents turn into crimes. Perversely, the ECC might be seen as a law enforcement competitor to Europol and would need to be sensitive to the possibility that the efforts from Europol to build up trust in the criminal justice community would be squandered by the ECC trying to establish its own name. The end result might be a sub-optimal situation for both Europol and the ECC since it would take time for the ECC to establish its credibility whilst Europol's might be undermined.

The ECC hosted at Europol would be just as capable of performing certain activities as under the option in which the ECC is owned by Europol. In terms of resources, an ECC hosted by but not owned by Europol would not require the reinvestment 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 ECC and Europol. The ECC might pay a sum each year (a percentage of the capital investment in these infrastructures) in return for which the ECC would be permitted to use the resources.

7.3.4 A virtual ECC

Given the differing competencies, perspectives and legal bases of each relevant organisation, there is also merit in consideration of a virtual ECC that tries to tie each relevant organisation together more strongly better to deliver an overall capability, without seeking to create a wholly new organisation. This would be immediately practicable since it would require fewer legal amendments. It might also secure political acceptability since it would not require the establishment of new structures or a new agency. A virtual ECC would also be much less resource-intensive to establish compared to the extensive set-up costs of a new data centre, intelligence machinery and forensic suite. This option constitutes an incremental increase from the option of maintaining the status quo.

Links and relationships with other stakeholders would need to be modified in relatively minor ways. For example, designing operational co-operation agreements between ENISA and Europol – which might require amendments to ENISA's governing regulation allowing it to process personal data. This would be less work compared to creating the legal basis for an entirely new organisation.

Given the broad nature of the activities articulated for an ECC (as indicated above), a Virtual ECC is attractive because it leverages the expertise and competency of each different organisation without requiring the recreation of capacity or capability.

Nonetheless, there are some significant operational drawbacks to a virtual centre. Not least is the fact that a lack of a centre of gravity of the ECC being hosted within a specific organisation may mean that many stakeholders view it as the "status quo" option. This would not necessarily be the case: despite the term "Virtual ECC" there would be resource implications in terms of establishing a small governance team (which would no doubt need to be sited somewhere). So a virtual centre would still incur some costs and might also be expected to sign similar 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.

7.4 Comparison of options

In the next sections we present an overview of each of the six factors associated with the feasibility of an ECC, namely its mandate (Section 7.5); the activities it would perform (Section 7.6); the resources available to it (Section 7.7); risks to its establishment and functioning (Section 7.8); aspects of co-operation (Section 0)and expected impacts (Section 7.10). We begin each section by describing the particular issue and then compare and contrast either the implications of this issue for each option, or the differences in how each option would address the issue. As indicated, with respect to some of these factors (especially the activities) the comparison may actually be clearer between the option of "maintaining the status quo" and "establishing an ECC" (regardless of whether that is via an ECC owned or hosted by Europol or a virtual ECC). In other areas (e.g. resources) there are clearer differences, for example, in how the costs might fall between each organisation playing a role in tackling cybercrime. At the end of this Chapter, an overall table for comparison is presented (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).

7.5 Mandate

The mandate of a future ECC governs what is within and beyond scope in terms of the types of cybercrime phenomena that the ECC should address. Scope may be defined according to severity, impact (across borders) or some other indicator. As we have seen, there is currently a wide degree of variation between the types of cybercrimes dealt with at national and European level. In general, we suggest that any EU-level support such as that the ECC might be expected to provide (in terms of strengthening existing MS capabilities) should focus on those issues that are pan-European in nature. Furthermore, what appears to be the evolving “post –organised, service-led” nature of cybercrime means that an ECC would need to be empowered to act to support Member State investigations into what may not necessarily fall into a legal definition of “organised”.

As we have seen, due to cross-border characteristics, complexity arises in respect of establishing the threshold when low-level incidents (e.g. reports of a phishing attack against a financial institution) become so prevalent as to become a cross-border concern (e.g. where that financial institution is based in a number of countries).

Finally, it is important to recognise the wide variation in approaches and understanding of what specifically constitutes cybercrime, we have seen in Chapters 2 and 3 that a minority of types of cybercrime are specifically where ICT systems are the target. Many other types of cybercrime reflect the evolving aspects of cyberspace in committing fraud or where there is an IT element to traditional forms of crime.

Our approach therefore suggests that in respect of the mandate, ECC resources should try (as a general principle) to generally focus on those forms of cybercrime that target or specifically exploit lack of cybersecurity in ICT systems. In respect of law enforcement efforts (and criminal law) there exists a range of efforts to address what we term as Type II and III crimes (such as the range of legislation and enforcement efforts dedicated to fighting fraud). We instead recommend that as a general principle, a focused approach to the deployment of ECC resources should be taken. In practice this means that training and professional development activities should cover broader types of cybercrimes, whilst the strategic intelligence work should by principle concentrate upon those crimes that exploit intrinsic vulnerabilities in ICT systems and which target ICT systems.

7.5.1 Maintaining the status quo

Under this option the existing mandate of the relevant organisations would evolve without any specific impetus concerning the establishment of an ECC. For example, the new Europol regulation is expected to be agreed shortly and it is reasonable to expect that cybercrime in some form or another will also continue to be defined within Europol's core competency. In addition, Europol may retain its reactive posture and despite recent amendments, continue acting only on the basis of a threshold in serious (or organised) crimes affecting two or more Member States (existing Article 4(1) of the 2009 Europol Council Decision).

7.5.2 An ECC owned by Europol

An ECC within Europol would have a mandate influenced by (if not explicitly taken from) Europol's existing or future mandate (which is being prepared). Currently, Europol's mandate covers types of crimes currently listed in Art 4(1) and the Annex to the Europol Council Decision (ECD). Europol has the requirement to cover "organised crime, terrorism and other forms of serious crime…affecting two or more Member States in such a way as to require a common approach by the Member States owing to the scale, significance and consequences of the offences." The Annex to the ECD additionally explicitly defines "computer crime" as one of these forms of serious crime.

We thus expect that an ECC with a mandate consistent with or a subset of that of Europol's would cover the serious and/or organised types of crime in the following types, using Europol's current AWF infrastructure as a proxy for this categorisation:

Table 7.1 Different activities addressed by Europol's current intelligence analysis

	Type of cybercrime	AWF
1	Cybercrime driven by financial gain	Cyborg
2	Online child exploitation	Twins
3	Payment card fraud	Terminal
4	Mass Market fraud	n/a[(1)]

Europol's remit now includes "serious" (as well as organised) crime. It is also important to note that Europol acts reactively – that is to say it does so upon request of Member States.

In this sense, the mandate of the ECC (as envisaged) can be based within Europol's core mandate and the tasks that Europol was established to undertake. As with the status quo option (and noting the evidence presented in Chapter 6 about how each Member State views cybercrime) a revision to the definition of computer crime may in any case be required. Modifications to the description of computer crime as currently contained in the Europol Council Decision might be required to establish more clearly the definition of the types of computer crime that Europol (and by definition the ECC) would be competent to address. Evidence from our earlier research in this study suggests that more precision in this definition would be useful both from the substantive perspective (e.g. to concentrate on what the Council of Europe representatives informally describe as crimes where computers or data are the target) and also from the perspective of qualifying conditions – in that the phenomenon of the digital underground defies definition as "organised", more accurately described as being "networked".

7.5.3 An ECC hosted but not owned by Europol

An ECC hosted by Europol may be able to expand its mandate but only in limited ways. This is because it would, by necessity, rely on supporting infrastructure of Europol that is currently established to cover certain aspects (stemming from Europol's own mandate). 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 an ECC (just focusing on one criminal marketplace) undoubtedly would 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 listed in any Annex. A legal instrument for an ECC would thus need to define the types of cybercrime which would be within its competency, such as Council of Europe Type I – Attacks against computer data and systems.

7.5.4 A virtual ECC

The mandate of a virtual ECC would be similarly complex and broad. This is because unlike an ECC at Europol, agreeing the mandate for a virtual ECC would require negotiation between the four main stakeholders to establish where there was enough overlap and consistency between the governing rules of each one, to be able to create a new mandate that would be compatible and serve to allow each relevant organisation to play its part. Alongside Europol's "serious and organised crime" remit, one would have to also negotiate how Eurojust's broader remit to provide a more generalised form of support would work. CEPOL also deals in generalised training for senior and middle-ranking officers (not necessarily on serious and organised crime – for example, CEPOL covers canine unit training). Finally, there would be significant complexities of taking into account ENISA's broad mandate. In addition to not having the status of an operational agency, ENISA's mandate does not have any comparable threshold to allow it to focus on "serious and organised" Network and Information Security (NIS) issues. 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 co-operation team helps to facilitate best practice across all types of CERT. Having said this, recent initiatives have been also specifically aimed at national/governmental CERTs that formally or informally act as a focal point for CIIP at the national level. The concern for "integrating" ENISA's mandate into that of an ECC would thus be to establish a suitable threshold where cyber attacks against Critical Information Infrastructures (implied in ENISA's current mandate) can be core business of the ECC.[31]

7.6 Activities

From previous data-gathering we have identified different types of activities that an ECC may either conduct or support. These are listed below. In addition there would be activities relating to the management and running of the operations of the ECC (classified below under the heading of governance). Some of these activities include some core criminal intelligence and law enforcement related tasks that are already being undertaken, but there also new activities, for example in the area of co-operation and co-ordination. These areas are:

- Governance of the ECC.
- Gathering sensitive criminal intelligence, providing analysis and investigative support to Member State-level investigations of cybercrime.
- Developing and delivering training, education and the sharing of best practice across the criminal justice community.
- Supporting co-operation, co-ordination, joint working and outreach (including fusion of strategic non-criminal intelligence analysis from other sources).
- Facilitating online cybercrime reporting –between law enforcement; between the private sector and law enforcement; and between citizens and law enforcement.

7.6.1 Governance of the ECC

Activities in respect of governance would include establishing the decision-making authority, drafting and preparation of documents (e.g. Terms of Reference and Mandate for the ECC Capability Board). It would also be necessary to formulate reporting structures to the governance bodies (e.g. Europol Management Board). Other tasks include:

- Answering queries from political oversight (e.g. COSI at the European Council and LIBE at the European Parliament).
- Supporting the work of the EUCTF by preparing documents between meetings as a way to build on the momentum from the initial start-up of the EUCTF.

[31] The revision of the 2005 ECI Directive is also considering the inclusion of the ICT sector alongside energy and transportation

- Identifying areas where the ECC could quickly demonstrate benefits to the Member States (common service catalogues in order to facilitate cheaper access to the market).
- Facilitating information exchange (e.g. preparing co-operation agreements; codes of conduct and MoUs between different stakeholders).
- Collecting and storing best practice from Member States.
- Drafting co-operation agreements with other non-criminal justice organisations such as CERTs, the private sector and other non-governmental organisations.
- Preparing an evaluation framework to monitor the effectiveness of the ECC and assess whether or not it is having desired impacts.
- Drawing up staff profiles for different types of personnel (e.g. profiles for the multi-source intelligence analysts at the Data Fusion Unit).

We introduce each of these activities briefly, before examining how they would be undertaken under each of the four options.

7.6.2 Gathering sensitive criminal intelligence, providing analysis and support to Member State-level investigations of cybercrime

Gathering criminal intelligence and supporting MS-level investigations on operations tackling cybercrime involves building on national-level capabilities (as already identified) and further strengthening the existing activities of Europol in this regard by planning for the workforce based on a better understanding of the scale of the problem. This would be possible by incorporating additional sources of intelligence. Presently, intelligence work includes the analysis of criminal data collected via the existing AWF infrastructure, with the aim of informing the creation of threat assessments that cover the evolving activities of those types of crime for which Europol is competent. It is important to distinguish between strategic and tactical intelligence. Strategic intelligence helps inform future understanding of threats and how the nature of the phenomenon is evolving (for example, new *modus operandi*). Tactical intelligence, on the other hand, is concerned with providing actionable intelligence upon which operations can be conducted – for example that a suspect is likely to be present in a certain location at a specific time. Tactical intelligence may also help with respect to investigative support.

The second core activity is in the realm of operational or investigative support. This can be addressed in a number of ways, including through strengthened provision of forensic capability to those Member States that do not have specific infrastructure or know-how. It also may require the bringing together of personnel from different Member States, collaborating on a common investigation in order to save time and improve efficiency – if personnel have the opportunity to be physically co-located then many hours may be saved on inquiries that normally might take months.

As we have seen, Europol currently conducts a set of activities including sensitive criminal intelligence gathering and the provision of operational investigative support to Member States with regard to serious and organised forms of cybercrime. This includes the analysis of intelligence via the AWF infrastructure. Europol can also deploy mobile forensic teams to Member States and can (assuming no link to SIENA exists in the destination country), link to Europol's information systems. Finally, Europol (in combination with Eurojust) provides a physical and administrative platform for Joint Investigation Teams (JITs) – a way to reduce inefficiencies in interaction by temporarily physically co-locating member state personnel in order to collaborate on investigations.

Our proposal is thus that the ECC should leverage the momentum and existing capability currently offered by Europol and Eurojust and not seek to "re-invent the wheel" by creating a competitor to Europol, with all the likely uncertainty that might result.

However, there is a discernable added value of utilising broader sources of information to this analysis: the private sector can have earlier knowledge of cyber-attacks which can be subsequently identified as criminal conduct.

Comparing how these activities might be performed across each of the options would seem to suggest that the main difference is between the degree of control and management that might be exercised. Under Option 0 (maintain the status quo) and Option 1 (a Europol owned ECC) it is possible to envisage relatively minor additional management burdens required to perform these tasks. Under Option 2 and 3, there would be some additional interfaces that would need to be created to allow a non Europol organisation to take a governing role over such a function (that currently exists).

7.6.3 Developing and delivering training, education and the sharing of best practice across the criminal justice community

The provision of training would need to include the basic and advanced levels of training (the "how") but also deeper education (the "why") to facilitate greater understanding amongst not only law enforcement but also the criminal justice community. Both such activities can support broad capacity-building at Member State level by maximising the chances that each police officer has a basic level of familiarity with the cybercrime environment. Furthermore, there is a need to expand the training and education efforts to all members of the criminal justice system, not just law enforcement personnel.

The European Police College – CEPOL

Our fieldwork consisted of discussions with CEPOL –the European Police College. In 2010–11 CEPOL's annual budget was €8.2 million. CEPOL training programmes are delivered and implemented within and by Member States and by organisations that are CEPOL's partners – there are over 40 partners across the EU – at least one in each Member State, including police colleges and universities. CEPOL offers grants to cover travel costs of those who attend training courses, but it does not fund or deliver those courses. It is part of the CEPOL model that the skills and expertise to deliver training come from the network of partners, facilitated by CEPOL.

In a similar way as with Eurojust, cybercrime activities in CEPOL are cross-cutting. Although there is no assigned full-time expert on cybercrime within CEPOL's 42 personnel, this is not necessarily unusual since the organisation operates as a platform to bring in content experts.

CEPOL has prepared 10 e-learning modules on cybercrime aimed at high-ranking police officers. Europol, ECTEG and the Member States have all been involved in the development of these modules.

European Cybercrime Training and Education Group (ECTEG)

During our fieldwork we learnt that the European Cybercrime Training and Education Group (ECTEG), established in 2001, possesses competency in the design, development and delivery of training for cybercrime law enforcement officials from the EU. To date ECTEG has been financed by the EU ISEC (Prevention of and Fight against Crime) Programme (from which, since its inception, it has received €4 million) and this funding model is regarded as unsustainable by those on the management board of ECTEG. ECTEG is run on a volunteer basis. The current Chair of ECTEG is the Head of the Irish High-Tech Crime Unit. UCD (University College Dublin) CCI (Centre for Cybersecurity and Cybercrime Investigation) offers an MSc in Forensic Computing and Cybercrime Investigation which has had input from ECTEG and under the Bologna Convention has received academic accreditation across other EU Member States.

According to publicly available data from 2010, Europol[32] indicates there were three five-day courses between February and June 2009 under Phase 1 of the training courses offered by ECTEG. In Phase 2 (under the MSc programme) there were nine five-day courses between September 2009 and November 2010 and two ten-day residential courses held at UCD CCI.

In 2010, Europol assumed a larger role in the running of ECTEG. Under the Europol programme, there were three five-day courses planned between January and October 2010.

It is important to note that unlike CEPOL, ECTEG is run on a volunteer basis and its "constituency" appears to be individual law enforcement officers. This can be compared to the CEPOL model, where CEPOL's constituents are police training colleges across the European Member States.

[32] Europol, Octopus Programme (2010)

Estimating demand for training

CEPOL's mandate is to cover senior and middle-ranking police officers across the EU (but it also has bilateral agreements with a number of non-EU countries. CEPOL indicated that it has run 10 activities specifically concerning cybercrime and 236 people have participated in these training courses.

ECTEG is understood to cover training of different types of law enforcement professionals involved in cybercrime. Data on students to the non-MSc-accredited portion of ECTEG training is unavailable. We understand that 28 students passed through the 2011 UCD MSc in Forensic Computing and Cybercrime Investigation. We did not find information about the degree to which these courses were subscribed (for example whether there was no space for further prospective students).

Apart from discussions at the Member State level and with Eurojust, we did not collect information on training with respect to judiciary or others in the criminal justice system (e.g. public prosecutors) working on cybercrime. However, as stated in the Internal Security Strategy and as noted earlier in this report, the ECC should aim to strengthen awareness and education of the judiciary in addition to law enforcement. We therefore envisage activities in this regard as expanding to include the training of the judiciary as a key stakeholder.

We propose training and education activities based along the lines described in Table 7.2 below.

Table 7.2 Types of education and training activities

	Type of training or education	Description	Delivery mechanism
1	Continuing professional development	This type of training would include both basic and continuing professional development. The training would be scoped around technical and procedural aspects (e.g. how to image a hard drive; how to undertake remote searches). The basic-level education aspects would be as broad as possible and aimed at all members of the criminal justice community (specifically public prosecutors and judicial authorities).	Five-day courses at students' own expense
2	Residential/academically accredited course in Cybercrime Investigation	Courses for education (the "why" of undertaking certain measures) enabling candidates to support broader strengthening of cybercrime capabilities at the Member State level. The MSc would primarily be aimed at law enforcement stakeholders and be accredited under the framework of the Bologna Convention.	Two 10-day residential courses per year with subsistence costs covered
3	Good Practice Exchange	A mechanism by which Member States and other relevant stakeholders (e.g. fraud investigators from the private sector) can exchange good practices, share experiences in a confidential and trusted forum.	Through the ECC Programme Manager collating outputs from the EUCTF between CTF meetings.
4	Continuous reference and e-learning	A shared, highly secured and electronically accessible resource supporting continual professional development, training and education efforts in addition to being an online source of reference material and community-driven platform for information exchange .	Through an e-LMS (Learning Management System) hosted on Europol's secured data centre or CEPOL's existing e-LMS infrastructure

We propose that the ECC Capability Board be responsible for conducting broad-based cybercrime training, available to all members of the criminal justice community. CEPOL is particularly important in this regard since it has an "enabling role" of being able to reach national police training colleges. This effort should build upon the role of CEPOL and the content and training legacy established by ECTEG, with CEPOL designated as the owner of training capability on the ECC Capability Board.

Comparing these set of activities across the different options reveals that Option 3 (Virtual ECC) might be the most complex in terms of training provision. Although Option 3 would easily be able to build upon training provision made by Cepol (and to a lesser extent ECTEG the additional complexity provided by the independence of the ECC (relative to the others) would present further risks in understanding roles and responsibilities. The same might be said for Option 2 (an ECC hosted by but not owned by Europol) since there would be additional complexity about roles and responsibilities and ownership of different aspects. Under Option 0, the currently disparate training and education arrangements might evolve to become further fragmented. Option 1 has the possibility to offer a clear ownership and home for cybercrime training and professional development, but at the expense of the potential for it to be biased toward law enforcement needs.

7.6.4 Supporting co-operation, co-ordination, joint working and outreach

Cybercrime is a complex phenomenon in that responsibility to tackle it falls across both the public and private sector, and information is often held or collected by the private sector on incidents (before it is possible to determine any law enforcement involvement) but also on crimes that either individuals or organisations may have witnessed. In the case of the latter they may or may not wish to involve law enforcement.[33] In addition, as has been noted, co-operation and co-ordination are also important in cross-border investigative activities between law enforcement from different Member States.

Whilst we recognise that the different mandates of various organisations present challenges for successful co-operation, the presence of the ECC Capability Board would help to ensure visibility of these concerns. This is particularly the case regarding co-operation with the CERT community.

In a focused sense, a pan-European LEA co-operation capability can support cross-border investigations by providing a temporary platform for direct collaboration, saving the national units time and effort. There are also aspects of co-operation with organisations outside the criminal justice community. Specifically these non-criminal justice organisations include CERTs, financial institutions, cybersecurity service providers, the CERT-EU and others such as the Anti-Phishing Working Group (APWG), Messaging Anti-Abuse Working Group (MAAWG), IMPACT and the Internaitonal Cyber Security Protection Alliance (ICSPA).

Co-operation and co-ordination constitute one of the most difficult areas to establish due understandably, to the interests and mandates of the respective organisations. In the way in which we interpret co-operation in the context of the activities of the ECC, we propose that this occurs at essentially two levels:

- At the national level, between different stakeholders in different Member States including national/governmental CERTs and national LEAs with the ECC providing a common framework (in terms of an EU wide cybercrime intelligence requirement, for example).
- At the European level between the LEAs and ECC. Although information sharing should formally take place between the LEAs and ECC, the use of a common information exchange framework would facilitate co-operation. One possible aspect would be that the national/governmental CERTs, with the advice of the Joint LEA-CERT PPP officer, would share information (according to the common information exchange framework) with the ECC via the national LEA capability.

[33] Possible reasons suggested by one interviewee from a Member State included: fear of damage; if the amount stolen was not enough; if the event had a chance to become public knowledge, etc.

At the purely EU level, the ECC would also interact with the EU-CERT in its defined role as being the CERT for EU institutions (e.g. the European Commission, Council but also other EU agencies such as Europol and Eurojust and the Carbon Trading Scheme).

The formal presence of ENISA on the ECC Capability Board would permit the strategic perspective of the national/governmental CERTs community to be taken into consideration, helping to encourage understanding between different stakeholders (especially in the non criminal justice domain).

Table 7.3 Overview of activities in the area of co-operation and co-ordination

	Co-operation and co-ordination mechanism	Description	Involved parties	Type of resource	Model/ proxy
1	Data Fusion Unit (DFU)	The collection, analysis, assessment and dissemination of relevant broad non-sensitive criminal intelligence from a wide variety of public and private sources. This Unit would also be responsible for preparing and disseminating product to the ECC stakeholders. It would also include a forward-looking technology observatory to monitor how new technologies would give rise to opportunities for crime.	Financial institutions; ISPs; national/ governmental CERTs; CERT-EU; security service providers; others (e.g. APWG)	Posts at the ECC	EMCDDA RTX Unit
2	Joint LEA–CERT PPP Network	The ECC offers to support funding for one law enforcement officer post to work physically alongside the designated national/governmental CERT in order to fulfil an EU-wide information-gathering requirement concerning cybercrime.	National/governmental CERTs	Funding from the ECC to MS	EMCDDA National Focal Points
3	European Cybercrime Resource Facility (ECRF)	A Unit tasked with supporting an extended office-hours one-stop-shop service allowing direct queries from all types of criminal justice stakeholder (with a specific focus on public prosecutors and judges) in Member States to be answered. The ECRF would not replace the provision of operational support already provided by Europol but constitute more of a strategic & policy level information and knowledge sharing resource.	All Member States	Posts at the ECC	EJN/EGN

Data Fusion Unit

An important activity will be to further facilitate co-operation by pulling together the current different sources of data and information. This role is crucial with respect to gaining a better understanding of the phenomenon (to inform better resource allocation) but also as a way to understand how patterns of cybercrime evolve. Co-operation and co-ordination at a tactical level may be sufficient if the aim is to prosecute more criminals. However, in order to get ahead of the evolving nature of cybercrime, the ECC should possess broader insight into levels, type and characteristics of incidents. Closer co-operation with certain stakeholders (particularly the network of pan-European CERTs) can support this.

We envisage that a similar number of personnel (seven) as currently reported working in the Reitox (RTX) Unit of the EMCDDA would be required to undertake activities relating to analysis of multi-source non-criminal threat intelligence. These analysts, whilst possibly possessing a similar skill profile to an analyst working on the first set of activities (criminal intelligence) would be also conducting broader strategic intelligence analysis on a range of other data sources (excepting that from the AWF infrastructure). These sources might include:

- Specific meta-information (of interest in a pan-European context) from an online incident-reporting tool deployed at Member State-level by law enforcement.
- Data from other non-European criminal justice and law enforcement partners such as the US Secret Service, law enforcement authorities in Russia or China or even information flows from Interpol's nascent new centre in Singapore.
- Data from the CERT Liaison Officers fulfilling a Common Intelligence Requirement to feed information back to the ECC.
- Direct reports from certain organisations, for example financial institutions or CSPs.
- Data from private-sector security service providers e.g. anti-virus providers; operating system companies or those who monitor and provide data on the relative "health" of cyberspace.
- Data from other NGOs, for example the APWG, MAAWG as well as research organisations CAIDA and TeamCymru.

It is important to note that these personnel have a different function from the analysts conducting analysis of criminal intelligence. The role of the postholders conducting activities in the DFU is to analyse and make sense of a broad range of information from sources outside of the very specific highly controlled and sensitive areas of criminal intelligence. These additional personnel are required because the sheer variety and complexity of data sources out there will require additional resource to make sense of them, in order to monitor emerging patterns in incidents (as they might evolve from reported incidents to become more clearly evidence of crimes). Furthermore as they would be receiving data from the CERT Liaison Officer Network (see below) they would necessarily need to be ready to cope with information flows back from the national/governmental CERT. Other activities this unit could undertake (in line with the findings from earlier aspects of this study) include the preparation of tailored intelligence products to Member States and keeping a "watching brief" on technological developments to understand and inform where new technology would provide new opportunities for criminal behaviour.

Joint LEA–CERT PPP Network

The second and supporting activity with respect to co-operation is the co-funding of a post at the Member State level to be physically co-located with the national/governmental CERT.[34]

We choose this particular type of CERTs (recognising, as Chapter 3 has shown, that there are many different types of CERT) for specific reason. National / governmental CERTs may be considered as the first amongst equals of CERT community at the national level. According to ENISA, they are:

- Concerned with incidents at the national level, affecting the 'critical information infrastructure'
- Can act as a national level contact point for incident management
- Often sit within a network of peers of other CERTs (e.g. CERTs within banking or telecommunications)

We recognise that the national/governmental CERT capability is still new. In late 2011 there were 23 national/governmental CERTs in existence across Europe.

This would be a kind of "mini Public–Private Partnership" (PPP). This post would not seek to supplement or overtake the role of the ENUs but rather provide additional capability on the ground to help information flow. The role of the members of the Joint LEA–CERT PPP Network would be to deal less in specific criminal intelligence information but rather fulfil a pan-European multi-source intelligence model with respect to incident data that national/governmental CERTs may be receiving from other peer CERTs in Member States. In addition the presence of increased capacity in this domain would also serve to broaden cybercrime capability at the Member State level. Noting recent work on CERT–LEA co-ordination there appears to be significant uncertainty about the legal basis for some CERT operations – therefore a law enforcement officer (who would be a seconded national expert from the Member State) would be knowledgeable about specific legal and operational aspects of information exchange.[35] Information flows would also (in the case of specific reporting of crimes for which the ECC was competent to act), go via the ENU to feed into intelligence-gathering activity.

It is crucial to note that the proposed Joint LEA-CERT PPP officer would not be a direct Europol employee (acting on behalf of the ECC) but rather a Member State law enforcement representative acting on behalf of the national level Law Enforcement

[34] ENISA Baseline Capabilities for National/Governmental CERTs Report (2010) for definition

[35] ENISA Legal Barriers to Information Exchange Report (2011)

community. This officer would also help fulfil an EU wide intelligence requirement by for example ensuring that incidents fulfilling particular criteria can be shared with the Member State level High Tech Crime capability and thence to the ECC.

A further activity of the CERT Liaison Officer would be to facilitate a better understanding of the operational and procedural constraints under which both law enforcement and non-law enforcement entities (e.g. CERTs) can share information. This could be achieved through the use of common "hypothetical" cases designed by the ECC Governance Team so that both partners could share information on an informal basis without fear of liability. Such mechanisms would need to be governed by a Code of Conduct or other measure that would be drafted, prepared and agreed by the ECC Programme Team.

In reality there might be two ways this support could be provided: either specific funding is allocated to assign a post from the Member State LEA to the national/governmental CERT or alternatively the funding could go to the designated ENU to establish such a role.

As practical examples of what the Joint CERT-LEA PPP officers might do, we envisage that the CERT-LEA PPP officer could provide law enforcement advice to the national/governmental CERT on procedures, and information on what sort of information can and cannot be shared, helping to facilitate information exchange (via the standards based reporting platform) between the national/governmental CERT, MS level law enforcement and the ECC. Other practical examples could be in providing a summary of cases meeting a certain criteria to the national level High Tech Crime function and thence the ECC.

We do not expect that this could result in further burdening of the national level high tech crime units but rather the additional capability represented by the Joint CERT-LEA PPP officer could facilitate smoother interaction between national level law enforcement and the broader cybersecurity community. because these personnel would come from (as in the Reitox model) national level they would be uniquely placed to both support the EU wide intelligence picture but also strengthen the activity of the national/governmental CERTs.

European Cybercrime Resource Facility

The final proposed co-operative activity under the auspices of the European Cybercrime Centre is the European Cybercrime Resource Facility (ECRF). We refer to the proxy of the European Judicial Network (EJN) and European Genocide Network (EGN) in this regard. Both are reported to have a small staff and their objective is to provide a platform for the sharing of knowledge and common solutions between public prosecutors and judicial authorities across the Member States. This knowledge-sharing is focused around achieving outcomes related to arrests and convictions. Evidence identified earlier in this study suggests that judicial authorities appear to be often the key (but underappreciated) link in the chain in terms of bringing as many criminals to court as possible. Therefore a peer network facilitated by the ECC would serve to help exchange information, common practice and knowledge in order to strengthen opportunities for prosecution of serious cybercriminals across the Member States. Again, the purpose of this network would not be to replace the Europol National Units, but to act as an additional platform for the exchange of Member State best practice across the broader criminal justice community (i.e. with a focus on the judiciary). The ECRF might also be able to strengthen the work of the EUCTF, by undertaking data-gathering activities at the behest of the EUCTF Chair to fulfil EUCTF requirements.

Comparing these activities across the options suggests that although Option 3 (Virtual ECC) has the potential for roles, responsibilities and accountability to be clear (since each organisation would be able to focus on their core tasks based upon an existing or slightly modified mandate) there would be significant complexity in setting up an institutional structure of the ECC, independent of each organisation but with responsibility for managing the interfaces between each organisation. By comparison, Option 1 and 2 would require institutional transition for an entity hosted or based in a law enforcement orientated organisation to undertake activities which require closer interaction and co-operation with non law enforcement stakeholders, particularly from the private sector and national/governmental CERT community. in the case of Option 1, this would require exploration of opportunities offered by the amendment of the Europol Council Decision to permit greater information exchange with the private sector, subject to appropriate controls concerning the use of personal data. Option 0 might evolve to situation of further fragmentation of co-ordination and collaboration efforts.

7.6.5 Facilitating online cybercrime reporting

The establishment and running of a reporting platform arguably is the most capital-intensive part of the envisaged tasks for a future ECC. The objectives of a pan-European reporting platform will be, ideally, to:

- Avoid overlapping investigations.
- Provide an indication of the landscape and support analysis of new criminal markets.
- Provide a means allowing the citizen to interact with Europol.

There are various Member States and third countries that have recognised the utility of an online reporting point to allow citizens to report instances of cybercrime. Furthermore, as has been envisaged by Europol, ICROS considers a more generalised approach as being a platform to permit reporting:

- From organisations (e.g. businesses) to law enforcement, for example as envisaged by ICROS via public and private access to the IFOREX (Internet and Forensic Expert Forum) experts exchange.
- From members of the public to law enforcement (via an online reporting tool on a website).

- Between law enforcement in different Member States (in particular the storage, sharing and automated data-transfer of information, which is understood to be currently under investigation by the ICROS Project Team).

It is important to distinguish that this system should have different information from other initiatives such as the proposed European Information Sharing and Analysis System (EISAS) and the mechanism currently provided for by Article 13a of the European Telecommunications Regulatory Package (ENISA, 2011c). This requires providers of publicly available telecommunications services to notify national regulators and ENISA of information security breaches. In an ideal world perhaps these systems might use the same infrastructure but the objective that each system is trying to achieve would be different. Nonetheless, some degree of interoperability might be sought and the DFU would seek to obtain inputs from such sources (as and when they become available) as an additional part of the broader (non-criminal) intelligence-gathering process.

One or two Member States indicated that the utility of such a mechanism remains questionable from the perspective of the generation of actionable intelligence. However, some benefit could be derived from this system (given the relatively small resources involved in setting one up) as a mechanism to reassure users of cyberspace and further support law-enforcement presence in cyberspace. Over time such a system might, eventually, also be a useful source to triangulate strategic intelligence received from Member States, the CERT community and other sources listed above.

However, evidence from our research (particularly from discussions at the scenario-based workshop of the 14th November 2011) suggests that there would be little appetite for an ECC to have its own public-facing presence on the Internet specifically related to citizen reporting. Therefore we formulate the activities concerning public reporting as having the character of supporting and facilitation.

The proposed activities would see the ECC commission the design, development, testing and implementation of a standalone reporting-point software application that could be used by Member States. This would be based around RfC 5901 e-Crime extensions to the extant IODEF (Incident Object Description Exchange Format) reporting standard (IETF, 2010). By doing so, this would enable the broadest possible integration and interoperability with incident reporting mechanisms in use in for example CERTs financial institutions and CSPs.

Comparing this activity across the different options suggests that the main differences would exist between Option 0 (maintaining the status quo) and the three other options where this activity takes place. In that respect, the Option which has the strongest approach to setting out roles and responsibilities for this activity would be the most preferred. This is because of the risks associated with managing ICT projects (requiring strong oversight).

7.6.6 Comparison of each option in undertaking ECC activities

Since, as we indicate earlier, each of the four options would enable these activities to take place (to a greater or lesser degree) we present a comparison table to facilitate review. This is based on an assessment of the relative strengths and weaknesses of how successfully each option would be able to conduct these activities, noting the descriptions of them provided above.

Table 7.4 Comparison of activities across the different options

Activity	Maintain the status quo	ECC owned by Europol	ECC hosted by Europol	Virtual ECC
Gathering sensitive criminal Intelligence, providing analysis and support to MS-level investigations of cybercrime	-/+	++	+	+
Developing and delivering training, education and the sharing of best practice across the criminal justice community	-	+	++	+
Supporting co-operation, co-ordination, joint working and outreach	-	+	+	++
Facilitating online cybercrime reporting	-	+	+	+

Source: findings of this report

Key (relative to the baseline of current situation):

–/+ the same

++ Significantly stronger

+ Stronger

– Weaker

– – Significantly weaker

7.7 Resources

The question of resources is perhaps one of the most interest to the policy community since the activities and mandate of an ECC must of course require some level of investment from the public purse.

In line with the scale of this work and its ex-ante nature, in this section we present broad comparisons of estimates for the resources likely to be required under each of the different options.

In order to perform the background analysis to consider how many resources (in terms of people or one-off or ongoing expenditure) we must first identify a series of inputs. These serve as the building blocks of this estimation exercise. These inputs can range from the average cost of employing personnel (which is different from the salary of the employee as it includes social security costs, etc. and thus represents the budget costs to an organisation) to the costs of acquiring IT equipment, paying for travel and subsistence for personnel to attend meetings, commissioning research or buying or using other products or services (e.g. translation or software development).

Table 7.5 below indicates these different types of resource:

Table 7.5 Types of resource considered

Item	Description
Labour	Costs to employ personnel for one year, including salary, pension, social security contributions, etc.
Non-Labour	ICT desktop equipment Training Travel and expenses Co-funding Services Software development Software maintenance Studies & Research Translation Design and communications

It is also important to note that there are types of resource we do not include or cover, in some cases for reasons following on from the assumptions we make in this study. Other types of resource are excluded because this exercise is focused on the set-up and preliminary phases of the ECC. These estimates also do not represent a detailed through-life cost estimate.

We do not consider rental of facilities since we assume that under each option, there is spare space available in facilities, for example the new Europol HQ. Similarly, we do not consider ongoing utility costs such as lighting, heating, water, electricity.

We do not include capital-intensive ICT infrastructure, since all of the options under detailed consideration at this stage are able to leverage in some way Europol's existing ICT infrastructure, such as the AWF system, Computer Forensic Network (CFN) and Data Centre.

We do not consider depreciation of items acquired. This is most notable with the purchase of ICT equipment, which can have a definite life span (after which new equipment would need to be acquired). Nor do we consider amortisation of capital expenditure; we assume that major capital expenditure is a one-off lump sum.

We also do not consider the Member State-level costs required to set up, for example additional IT systems where there was no connection to Europol's information systems via SIENA.

Finally there may be costs associated with technical connections to pan-European intelligence-sharing networks that might be required, which are not considered.

7.7.1 Allocation of costs

Across the types of activities that are envisaged for the ECC, we can allocate these costs as laid out below in Table 7.6:

Table 7.6 Types of cost for each activity

Activity	Labour	Non-Labour
Governance	Costs of staff to fulfil the governance function of running the ECC, supporting the ECC Capability Board and providing general administrative support	ICT desktop equipment, travel and expenses; services; studies and research; design and communications
Gathering sensitive criminal Intelligence, providing analysis and support to MS-level investigations of cybercrime	Costs for trained intelligence analysts to analyse criminal intelligence data and provide ongoing operational support to MS level law enforcement	ICT desktop equipment; services
Developing and delivering training, education and the sharing of best practice across the criminal justice community	Costs for one expert to update training course suitable for broader criminal justice community	Training; travel and subsistence; studies and research; translation
Supporting co-operation, co-ordination, joint working and outreach	Costs of staff for the Data Fusion Unit, and to run the European Cybercrime Network	ICT desktop equipment; co-funding; studies and research; translation
Facilitating online cybercrime reporting	n/a	Software development; software maintenance; studies and research

7.7.2 What are the main drivers of cost?

As has already been indicated in the introduction to this section no new capital investment of a building or large ICT infrastructure is required in any of the options under detailed consideration.

The major cost drivers for each of the options under consideration in this chapter are labour costs, specifically for Europol trained criminal intelligence analysts to perform intelligence and operational support tasks. As has been shown in Chapter 2, the uncertainty about the real scale of the problem means that we cannot easily determine how much labour would be required to meet demand. Predicting workforce estimates for intelligence analysis in the domain of cybercrime is complex – some cases may take many months of work requiring the time of several analysts if the technical aspects prove complex. Therefore to provide support for decision-makers, we frame the estimate for the personnel associated with the second set of activities: providing criminal intelligence analysis of sensitive data and operational support to Member States on the basis of two workload requirements of "high" and "low" representing an increase of additional personal from what were the complement of this type of activity in June 2011:

- "Low workload requirement" – an additional **21** personnel (14 functional posts and seven support posts) on top of the reported June 2011 complement of Europol personnel working in criminal intelligence and operational support.
- "High workload requirement" – an additional **240** personnel (158 functional posts and 82 support posts) on top of the reported June 2011 complement of Europol personnel working in criminal intelligence and operational support.

We will return to these scenarios in Chapter 8 on the Implementation Plan.

Furthermore, none of our options require additional capital investment on behalf of Member States, for example by requiring Member States to invest in additional resource for connections to the SIENA communications network.

In the other domains, the number of personnel required is less sensitive to the scale of the problem. For example, for the governance team, experience from other organisations illustrates that a minimum of two functional personnel would be required, regardless of the scale of the phenomena. If the number of trips and effort that the governance team would need to formalise information-sharing arrangements with other stakeholders both in Europe and aboard is taken into account, then we might expect that two functional officials (head and a programme officer) would be required with an administrator to support them.

7.7.3 Interpreting the data

The consideration of resources was just one aspect of the evaluation model. With this in mind, the broad resource estimates that follow should be considered primarily for the pre-start task of identifying the likely high-level appropriations. These indicative costs do not constitute a detailed bottom-up budget and should not be used to plan or budget for a new ECC. Rather the intent is to give an appraisal of the likely implications that can be set alongside the other factors (noted in the introduction to this chapter) that contribute to an evaluation of the feasibility of an ECC. Finally, we have arrived at the values in the estimate via a combination of different methods – for example, by using other organisations as a proxy or by calculating present-day costs from data from 2008. Except where explicitly stated, these estimates also represent averages. In preparing this estimate, our study team worked according to the principle of proportionality, weighing the need to allocate resources in the study to a number of different tasks (not just the estimation of costs). Even in this feasibility assessment phase of the study, consideration of the issue of how resources affect the feasibility of establishing the ECC was only one of the considerations.

7.7.4 Sources of the data

Many of these estimates use different data sources. It is important to understand the source when interpreting these data. The sources have been either explicitly mentioned or used as a basis for extrapolation. In this section we elaborate on the provenance of the inputs – namely what sources have been used to develop the estimates. Further detail can be found in the table in Appendix F. The sources include:

- Data provided as part of this research exercise (e.g. numbers of personnel doing similar or related activities in Europol, Eurojust, ENISA etc).
- Calculations from the EU's own 2008 budgetary fiche for annual resource implication for different types of personnel.
- Proxies such as the EMCDDA, European Genocide Network (EGN).
- Published budgets from different relevant agencies including Europol and CEPOL.
- Data provided to us by relevant organisations for example Europol, Eurojust and ENISA.[36]

7.7.5 Comparison

In the next section we compare the resource implications of each option, starting with maintaining the status quo (Option 0).

Option 0 – Maintaining the status quo

Table 7.7 below indicates the summary of estimated resource implications for the status quo. Detail on what makes up these items is located at Appendix F.

Table 7.7 Overview of resource estimates for option 0

	One-off expenditure (€)		Ongoing expenditure (€)	
	Labour	Non-Labour	Labour	Non-Labour
ECC governance	n/a			
Criminal intel analysis and operational support			3,700,000	
Broad-based training, education and best practice				4,000,000
Co-operation and co-ordination			400,000	

[36] For example, Europol File no. 2720–29 (2011)

Online reporting platform	200,000

The assumptions in this option are based on our current understanding of the present situation.

Option 1 – ECC hosted by Europol

Table 7.8 below indicates the summary of estimated resource implications for the ECC under Option 1, including a percentage for programme risk at 5%. Detail on what makes up these items is located at Appendix F.

Table 7.8 Overview of resource estimates for option 1

		One-off expenditure (€)		**Ongoing expenditure (€)**	
		Labour	**Non-Labour**	**Labour**	**Non-Labour**
ECC governance				400,000	300,000
Criminal intel analysis and operational support	Low workload requirement		86,000	2,800,000	
	High workload requirement		960,000	31,500,000	
Broad-based training, education and best practice	Low workload requirement				800,000
	High workload requirement				6,400,000
Co-operation and co-ordination			100,000	1,100,000	1,600,000
Reporting Platform		300,000	200,000	50,000	
Other (security)					300,000

The assumptions underlying the cost model in Option 1 are as follows. We assume that the additional funds would go to Europol to be deployed according to the Implementation Plan for the ECC. The ECC Capability Board (see Section 8.1 below) would be the means by which each stakeholder would help to ensure that the funds were distributed to activities of the ECC appropriately.[37] We assume that all personnel (both in the governance team, DFU and ECRF) would be recruited to the "Restricted" level at Europol. It is also based on the assumption that a private-sector firm would be tasked with developing the reporting platform. We also assume that training is delivered by EU-level law enforcement specialists and not seconded national experts. We assume that space is available at EHQ for the additional personnel (under both scenarios) and that the costs of security, catering, and so on are covered.

[37] In reality this would mean the only organisation to see its budget shifted would be ECTEG, which is an informal organisation. CEPOL would continue to support training activities e.g. through its online platform.

Option 2 – ECC owned by but not hosted by Europol

Table 7.9 below indicates the summary of estimated resource implications for the ECC under Option 2, including a percentage for programme risk at 5%. Detail on what makes up these items is located at Appendix F.

Table 7.9 Overview of resource estimates for option 2

		One-off expenditure (€)		Ongoing expenditure (€)	
		Labour	Non-Labour	Labour	Non-Labour
ECC governance			12,000	400,000	900,000
Criminal intel analysis and operational support	Low workload requirement		100,000	3,200,000	600,000
	High workload requirement		1,000,000	31,900,000	
Broad-based training, education and best practice	Low workload requirement				800,000
	High workload requirement				6,400,000
Co-operation and co-ordination			100,000	900,000	1,600,000
Reporting Platform		100,000	200,000	30,000	
Other (security)					300,000

The assumptions in this option are as follows. We assume that unlike Option 1, under this option, the ECC would get its own ring-fenced budget to assign to activities. We assume that in order to obtain the use of Europol's ICT infrastructure, payment of an annual service charge (assumed to represent 1/12th of the total reported one-off costs of such infrastructure) would be required from the ECC budget to Europol.

We assume that not all posts require Restricted Status and seconded national experts would work in the DFU and ECSF under this option. We also assume that the broad-based training, education and professional development activities can be delivered by seconded national experts. We further assume that the online reporting platform is designed, tested and implemented by a not-for-profit organisation rather than a commercial third party. This also holds for the support of this platform.

Option 3 – Virtual ECC

Table 7.10 below indicates the summary of estimated resource implications for the ECC under Option 3, including a percentage for programme risk at 5%. Detail on what makes up these items is located at Appendix F.

Table 7.10 Overview of resource estimates for option 3

		One-off expenditure (€)		Ongoing expenditure (€)	
		Labour	Non-Labour	Labour	Non-Labour
ECC governance			12,000	400,000	900,000
Criminal intel analysis	Low workload		100,000	2,800,000	600,000

and operational support	requirement				
	High workload requirement		1,000,000	31,500,000	
Broad-based training, education and best practice	Low workload requirement				700,000
	High workload requirement				6,200,000
Co-operation and co-ordination			100,000	600,000	1,600,000
Online reporting platform		100,000	200,000	30,000	
Other (security)					300,000

Under this final option, we assume that each contributing organisation receives additional resources as per the allocation below to deliver their activities. We assume that the independent ECC governance team would in all likelihood physically use Europol HQ offices, but have a separate ring-fenced budget. Other relevant agencies (see below) would receive additional resources to fulfil the activities of the ECC. Table 7.11 details how we expect these might be spread.

Table 7.11 Spread of resources between relevant organisations in the virtual ECC option

	Virtual ECC					
	Europol (€m)	**Eurojust (€m)**	**Cepol (€m)**	**ENISA (€m)**	**Other (€m)**[38]	**ECC(€m)**
One-off costs (low workload requirement)	0.08				0.27	0.01
One-off costs (high workload requirement)	0.96				0.27	0.01
Ongoing costs (low workload requirement)	3.5	0.5	0.74	0.3	0.03	2.9
Ongoing costs (high workload requirement)	32	0.5	6.2	0.3	0.03	2.9

The remaining assumptions in this option are identical to those for Option 3. We assume that in order to obtain the use of Europol's ICT infrastructure, payment of an annual service charge (assumed to represent 1/12th of the total reported one-off costs of such infrastructure) would be required from the ECC budget to Europol.

We assume that not all posts require Restricted Status and seconded national experts would work in the DFU and ECSF under this option. We also assume that the broad-based training, education and professional development activities can be delivered by seconded national experts. We further assume that the online reporting platform is

[38] e.g. an NGO such as under the Safer Internet programme

designed, tested and implemented by a not-for-profit organisation rather than a commercial third party. This also holds for the support of this platform.

7.7.6 Overall comparison

Appendix F provides a full overview of these costs based on our assumptions broken down by activity and then capital and operational expenditure.

Our qualitative assessment of these costs is provided below at Table 7.16.

Table 7.12 Comparison of options in terms of resourcing

Cost line	Maintain the status quo	ECC owned by Europol	ECC hosted by Europol	Virtual ECC
ECC Governance team	No additional funding	Europol receives additional funding to allow it to set up and govern the ECC and the ECC Capability Board	ECC receives its own funding Europol receives additional funding to cover costs of use of infrastructure by ECC	ECC receives its own funding Europol receives additional funding to cover costs of use of infrastructure by ECC
Sensitive criminal Intelligence & operational support	Europol continues to receive funding based on its own assessment of requirements	In due course, Europol receives additional funding in line with low/high estimates to assign to sensitive criminal intelligence and operational support, via the ECC Capability Board	ECC receives its own funding In due course, Europol receives additional funding in line with low/high estimates	In due course, Europol receives additional funding in line with low/high estimates
Broad-based training and professional development	CEPOL resourcing continues as per present; ECTEG programme resourcing continues under Europol	Europol receives funding to assign via ECC Capability Board to broad-based training and professional development	ECC receives funding direct to assign to broad-based training and professional development via CEPOL	CEPOL receives additional funding to deliver broad-based training and professional development
Co-operation and collaboration	ENISA funding continues as present; activity is also resourced via Europol (e.g. via IFOREX)	Europol receives funding to assign via ECC Capability Board to activities of the Data Fusion Unit, ECSF and Joint LEA–CERT PPP Network	ECC receives funding direct for activities of the Data Fusion Unit, ECSF and Joint LEA–CERT PPP Network	ENISA receives funding to permit facilitation of Joint LEA–CERT PPP Network Eurojust receives funding to permit facilitation of the ECSF
Development of an online reporting system	n/a	Europol receives funding to assign via ECC Capability Board to commission an online reporting platform	ECC receives funding direct to commission an online reporting platform	NGO is commissioned independently to develop an online reporting tool

Table 7.13 below presents a summary of the expected resource implications across the three options requiring new resources. We also include in the totals provision for project and programme risk at 5% of the total ongoing cost.

Table 7.13 Comparison of estimated overall annual resources

Option:	Europol owned ECC (€)	Europol hosted ECC (€)	Virtual ECC (€)
Ongoing labour costs (low workload requirement)	4,350,000	4,530,000	3,830,000
Ongoing labour costs (high workload requirement)	33,050,000	33,230,000	32,530,000
Ongoing non-labour costs (low workload requirement)	3,000,000	4,200,000	4,100,000
Ongoing non-labour costs (high workload requirement)	8,600,000	9,800,000	9,600,000
Total ongoing costs (low workload requirement)	7,350,000	8,730,000	7,930,000
Total ongoing costs (high workload requirement)	41,650,000	43,030,000	42,130,000
Total ongoing costs inc. risk (low workload requirement)	**7,750,000**	**9,130,000**	**8,330,000**
Total ongoing costs inc. risk (high workload requirement)	**43,750,000**	**45,130,000**	**44,230,000**

7.8 Risks

We identify a number of risks related to the feasibility of the ECC. Chief amongst these is the risk of establishing a new organisation in such a complex area beset by many reporting chains and relationships between different stakeholders, each with their own mandate.

- Political acceptability to Member States: the Member States will see powers being taken away from them rather than the ECC supporting their activities.
- Visibility to all stakeholders: that the ECC may be seen as visible to all the stakeholders across the criminal justice and law enforcement community addressing cybercrime – chiefly the private sector (CERTs and other relevant institutions such as ISPs and financial institutions) and law enforcement partners across the globe (for example, Interpol, and agencies in the United States, Russia and China).
- The risks of confusion: these could arise from institutional complexity, which may result in overly long negotiations about who has the competence or responsibility to act in one area, leading to possible situation where no one takes responsibility and concerns or issues fall between the boundaries of each organisation.

- The risk of organisational inertia: this reflects the possibility that it would be difficult to account for resources allocated to any organisation involved in the ECC. This is particularly the case where it is difficult to "ring-fence" resources specifically to go toward the operation of the ECC.
- Programme and project management risks: finally, as with the introduction or establishment of a new organisation, there may be management risks which may not be visible at the outset – for example, untoward circumstances or unknown issues that surface once the programme has been embarked upon which may result in cost overrun.

As with activities, since the risks are visible regardless of which option is selected, we present an overview comparison table instead of an extensive description of differences. Table 7.14 represents our evaluation of the risks.

Table 7.14 Comparison of options in addressing risks

Risk	Maintain the status quo	ECC owned by Europol	ECC hosted by Europol	Virtual ECC
ECC is not accepted by Member States	-	+	+	-
Lack of visibility to all stakeholders	-/+	++	+	--
Institutional complexity	-/+	+	-	--
Organisational inertia	--	-	++	+
Programme and project risk	+	-/+	-/+	-/+

Key (relative to the baseline of current situation):

++ Significantly stronger at managing the risk

+ Stronger at managing the risk

–/+ Equal to current capability to address the risk

– Weaker at managing the risk

– – Significantly weaker at managing the risk

In any respect, as good risk management practice with such large scale programmes introducing new capability or structures, it would be necessary to carry out a more formal periodic review and evaluation of progress (for example after the first year of operation) to help raise the visibility of any issues learnt in the first stages of the operation of the ECC.

7.9 Co-operation and collaboration between the ECC and other organisations

As we have seen throughout this study, co-operation and collaboration is regarded as one of the most important aspects and where the ECC could add the most value. There are different types of co-operation, however, involving a number of different types of organisation from both the public and private sectors.

In considering these different kinds of co-operation, firstly we may consider co-operation within the specific law enforcement community in Europe. Generally this co-operation is aimed at either achieving efficiencies in cross-border investigations or sharing of best practice or information. Related to this form of co-operation with respect to investigative support at Member State-level is co-operation between different stakeholders in the criminal justice community – notably law enforcement and public prosecutors. This is normally achieved through Europol and Eurojust Joint Investigation Teams (JITs).

Co-operation may also take place with other law enforcement and criminal justice communities outside of Europe – namely via Interpol and national-level organisations, for example in the United States (e.g. the USSS) Russia and China. This type of co-operation is particularly important given the way in which technology can enable cross-border criminal activity. Such co-operation may be crucial to prosecuting successfully criminals based overseas, but the negotiations and agreements over Mutual Legal Assistance Treaties (MLATs) and extradition requests may take time.

Finally there is co-operation and co-ordination with the private sector. As we have seen in Chapter 3, there are different players in the private sector. These include financial institutions (who may be indirectly victimised), ISPs (who may be able to spot incidents) CERT teams (who have a more detailed handle on how incidents are evolving) and others (e.g. not-for-profit groups or security service providers). Co-operation with the private sector might also take place at two levels – either in the realm of an investigation (e.g. working with hosting companies to permit access to servers) or at strategic level (e.g. taking in data from the private sector to understand better the relative levels of security in cyberspace and where likely threats may arise from).

In general, co-operation with the private sector concerns the objective of encouraging the sharing of information between the criminal justice community and the private sector. Very often this comes down to addressing or managing the motivation of the private sector to withhold information lest it be used by a competitor to derive economic advantage.

7.9.1 Models of co-operation

In addition to the information provided to us by Member States and the EU level agencies concerning co-operation based activities, we reviewed a number of co-operation models including those of the BCCENTRE, 2CENTRE and the EMCDDA to identify some characteristics about what approaches work for co-operation. Some of these examples focus on a more research based approach but they all include gathering together of expertise from different stakeholders. Each co-operation model builds upon the idea of sharing information and practices and styles itself generally as a platform with partnership working as a key facet of activities. We describe these in Appendix E.

7.9.2 Comparison

Under this option existing co-operation activities would likely continue with ongoing co-operation between Europol and Eurojust as part of Joint Investigation Teams. Furthermore, Europol would be expected to continue to work on concluding both operational and strategic agreements with other parties both in non-EU countries and the private sector. Europol is also known to be formulating increased co-operation with ENISA via a Liaison Officer placed at the Europol HQ. Finally, it is understood Europol has been working on co-operation with various private sector stakeholders including security service providers. ENISA for its part (as the other major stakeholder undertaking such activities) has its CERT relations team.

An ECC owned by Europol

Under this option, the additional resources proposed (under the RTX Unit model) would allow co-operation to occur a systematic basis under an ECC housed within Europol. Although modifications to the governing instrument of Europol might be required in order to allow deeper co-operation with the private sector specifically (since the current governing instrument permits only strategic co-operation) there would be significant synergies in leveraging current co-operation activities underway at Europol and between Europol and other organisations involved in criminal justice (e.g. Eurojust and via Europol's Platforms for Experts).

An ECC hosted by Europol

Under this option, the potential opportunities would be the same as above. However, the complexity of establishing a legal instrument to govern the activities of an ECC hosted by Europol would probably incur further confusion. For example, strategic co-operation agreements, such as those already signed between Europol and the private sector, would need to be re-written and agreed anew for the ECC. The financial implications of such co-operation would perhaps be clearer (particularly with respect to funds coming from a separate ECC budget going to national-level Liaison Officers who would be co-located with national/governmental CERTs.

A virtual ECC

Establishing co-operation between a virtual ECC and other stakeholders as described above would be even more complex. This is because the virtual ECC would need to take note of co-operation mechanisms established by each stakeholder and then try to map out where similarities and differences exist given the specific objective of each type of co-operation. This would be highly complex –for example, both Europol and ENISA have relationships with the private sector of varying degrees of maturity and so a decision would need to be made on which would take primacy and represent the ECC.

7.10 Impacts of the ECC

As noted in Chapter 2, it is very difficult to estimate the existing impact of cybercrime, let alone predict future impacts given different law enforcement configurations. Figures from industry on the nature and extent of cybercrime are not transparent in the way they are collected, and certain industry sectors may be motivated to increase the perceived scale of the problem to sell more products.[39] Figures based upon recorded offences may represent a function of law enforcement capacity and numbers or effectiveness of law enforcement personnel, rather than being correlated with the scale of the problem. In pragmatic terms, it was reported to us during the fieldwork for this study that no amount of additional law enforcement officers would ever eliminate cybercrime. However, our interviewees reported, in their expert view, that there is currently an imbalance between the extent of the problem and the resources dedicated to addressing it. Therefore we operate on the assumption that increasing the current capability would have some positive impact. However, we caution against over-reliance on current data about the prevalence of cybercrime to allocate resources or measure impacts.

7.10.1 Estimating cases that an ECC could handle

Table 7.15 below presents a simple estimate of how many cases it might be possible to run, per year, based on the zero, low and high estimates for personnel working in criminal intelligence and operational support activities of the ECC (these activities are common to each option).

According to publicly available data, in 2011 Europol ran around 12,000 cases.[40] Using figures from Europol's 2011 Work Programme[41] there were in total 231 personnel who could be expected to be directly or indirectly involved in working on these cases (137 personnel working toward Goal 1: EU Support Centre and 94 working toward Goal 2 – EU Criminal Intelligence Hub). Evidence from our study indicates that in June 2011 there were 23 personnel working across goals in the domain of cybercrime. Using this as a

[39] This is somewhat being undermined by new services which have security "bundled in" (for example, cloud computing service offerings where anti-virus filtering is performed "in the cloud", reducing the need for customers to purchase separate standalone anti-virus products.

[40] Europol, *European Investigator* (2011)

[41] Europol Work Programme 2012 (2011)

starting point we can then extrapolate the following figures described in Table 7.15 with respect to possible impacts using different levels of capacity.

Table 7.15 Estimated possible number of cases based on workload

Scope/activity	Total personnel*	Cases (p.a.)*
All Europol forms of serious and organised crime	231	12,000
Current Europol High-Tech Crime Centre (HTCC) capacity of criminal intelligence and investigative support	23	*1195*
ECC zero increase in capacity of criminal intelligence and investigative support	23	*1195*
ECC 'low' workload requirement of capacity of criminal intelligence & investigative support	*37*	*1922*
ECC 'high' workload requirement of capacity of criminal intelligence & investigative support	*181*	*9403*

Estimates in italics

7.10.2 Estimating outputs for a pan-European reporting point

The other area where we are able to estimate outcomes is in respect of a pan-European reporting point. We extrapolate from known data on traffic of reports provided as part of a 2008 data-gathering exercise run by OCLTIC. This exercise asked Member States to provide estimates of the number of reports per month received by their national reporting point, if one existed. This derives an estimated number of reports, per month of 10,712 across the EU. Over the course of a year, this totals up to 128,544 reports per year. In Table 7.16 below we compare this figure to publicly available data from the US Internet Crime Complaint Center (IC3) and the Anti-Phishing Working Group.

Table 7.16 Comparison of possible traffic to a public-facing reporting system

United States			Europe			Worldwide	
% pop online(a)	Number of reports received by IC3	Av per month	% pop online(a)	Number of estimated reports	Av estimated per month	Number of reports received by APWG(b)	Av estimated per month
77.3%	303,809	25,317	58.3%	*128,544*	*10,712*	*1,000,000*	*83,333*

Sources: (a) Internetworldstats – as of 16 Februrary 2012: http://www.internetworldstats.com/stats4.htm (b) Personal Communication Peter Cassidy, 2nd December 2011

There might also be more intangle impacts too. An example might be the increased visibility by citizens of cybercrime capability (this could be measured by questions in regulatr Eurobarometer opinion polls) or reduced victimisation (which might be captured by a pan European victimisation survey). Other impacts might include satisfaction of cybercrime police in working with their opposite numbers in other countries but also across the public-private sectors. This may also apply to cross border collaboration with partners outside the EU (both third countries but also other organisations like Interpol). The contribution of the ECC to improving co-operation and collaboration might be understood in terms of the time it takes to exchange and have cross border requests for assistance actioned, or the

7.10.3 Comparison of impacts

Again, due to the general commonality of the impacts across each of the options where an ECC is established, we present the comparison according to either maintaining the status quo or setting up an ECC.

Maintain the status quo

Using the two output-related measures provided above, we can see that under the option of maintaining the status quo, the number of cases attributable to the existing HTCC capability might remain comparable to current levels (not accounting for either any uplift in staff or increased effectiveness or efficiency of staff). In addition, impacts would revolve around existing segmented approaches with respect to intelligence analysis and investigative support. Each organisation would continue its activities with respect to gaining a better understanding of the picture of cyber(in)security and the way in which that maps to criminal opportunities.

With respect to the online reporting platform, since many nations continue to run such systems (e.g. the French Pharos system, the UK's Action Fraud or new proposed cybercrime reporting platform or the Italian CNAIPIC website) we might expect to see similar degrees of fragmentation across different approaches using proprietary standards and systems with little regard for interoperability. Furthermore, even at European level there is fragmentation: witness the efforts made on the ICROS initiative by Europol, together with the EISAS (European Information Sharing and Alerting System) and the Article 13 Data Breach Reporting framework. All of these initiatives revolve around the transmission of information relevant to tackling cybercrime but all are being run by different stakeholders. It might be expected that under the status quo option these efforts would continue in a separate way.

Under the option of establishing an ECC, we might see that it would be possible to work an increased number of cases, depending upon the extent to which increases in criminal intelligence and operational support functions were supported according to either the low or high model. This increase, however, would be very much determined by the effectiveness of some of the other activities – specifically concerning co-operation and co-ordination between criminal justice communities and the private sector. By establishing better co-operation with the private sector it would be possible to obtain more extensive and higher quality insight into the phenomena of cybercrime, leading to a more comprehensive information picture on the state of incidents and reported/unreported crimes.

7.11 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 Co-ordination and co-operation (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 Co-ordination and co-operation (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 Co-ordination and co-operation (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
Co-operation	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 co-operation with private sector – at present Europol co-operation with the private sector is via liaison and limited to strategic co-operation because of data protection requirements	An ECC hosted at but not owned by Europol would be able to create deeper and more substantive co-operative 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 co-operation 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	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.

	“bounded” crime type in and of itself – known as mainstreaming.	

7.12 Conclusion

Our recommendation based on the above assessment is that the most feasible option, given the mandate and the tasks that an ECC must undertake is for the <u>ECC to be owned by Europol</u>. Such a recommendation is based on a qualitative understanding of the likely risks and "least worst" aspects of the feasibility. This is in essence an argument between the implications of the organisational complexity of the "ECC hosted by but not at" option versus the risk under the "ECC owned by option" that the natural organisational inertia would see the ECC lose visibility amongst Europol's other activities. In the end, we judge that this latter risk is the lesser of the two.

In addition to representing the least worst choice in terms of the above organisational risks, there are certain distinct benefits to the proposed option. These include: an ECC owned by Europol would be able to leverage the existing extensive capital investments, the well-known brand of the agency and the complex and unique data-protection arrangements with regard to the further processing of personal data for criminal intelligence purposes.

In Chapter 8 we describe routes to how this might be implemented, based on some common principles derived from earlier findings and conclusions of this study and provide an indication of routes to implementation, noting the current climate of austerity and the risks identified in the above analysis. We also detail an arrangement enabling the different stakeholders (Member States, Eurojust, CEPOL, ENISA, etc.) to have a say in the overall delivery of a pan-European Cybercrime capability that the ECC would support, via the creation of a Capability Board structure, central to the ECC's role in tying together the different facets of a pan-European cybercrime capability as described in Chapters 4 and 5.

CHAPTER 8 Implementing the ECC

This final chapter describes how the recommended option, an ECC owned by Europol and seen as being the most feasible, may be taken forward. It notes the evidence identified throughout this study and a number of other important contextual factors such as the current climate of budgetary austerity.

The complexity of this domain requires that the preferred option indicated above cannot be simply "brought into being" instantaneously. According to the policy agenda, the ECC must be established by the end of 2013. In addition, the current climate of public-sector austerity means that there is extensive pressure to do more with less and, in addition, reduce in real terms budgets and staffing.[42]

Added to this is the fact that, historically, major public-sector programmes of this nature have been seen to be highly optimistic in their initial estimates of the cost, ranging from 10 to 200 percent according to estimates from the United Kingdom.[43]

Finally, linked to the current climate of public-sector austerity, there are challenges with respect to the political perception of how a new organisation might be viewed by European citizens at a time when there are demonstrations and protests across EU Member States concerning austerity measures.

Nonetheless, despite these aspects, policy interest in tackling cybercrime is high – for example, in 2011 the UK announced a programme of £650 million over four years under the National Cybersecurity Strategy. Out of this, €65 million (£63 million) would go toward cybercrime (Home Office, 2011). Therefore investment decisions must be placed in the context (outlined in Chapter 2) of the possible implications and damage to the economy and society posed by cybercrime.

Noting these factors, we have prepared this summary of an implementation roadmap intended to guide decision-makers in the further development of the ECC.

This further reflects the consideration from the Expert Workshop held in November 2011 that, viewed through the prism of a staged implementation, the options described in Chapters 6 and 7 are not necessarily mutually exclusive. What may start out as an ECC under one option, might, over time, evolve into something different. In order to provide

[42] It is understood that EU institutions have been told to reduce headcount by five percent by 2020

[43] See, for example, Mott MacDonald (2002)

some flexibility to policy-makers we therefore present a set of unambiguous principles that should govern the implementation of the ECC.

We also frame our discussion in the terms of a broader context concerning the delivery of capability to address serious types of cybercrime. This broader understanding is reflected in the widespread types of activities that have been identified as important to tackling this problem:

- Training and education of those involved in addressing cybercrime – both law enforcement and judiciary at different levels from basic first-responder training to real-time traffic analysis and training by industry.
- Organisational structures for providing operational support and trend analysis.
- Operational guidance and best practice on processes and operational matters such as remote searching, seizures and covert operations.
- Technology and infrastructure – such as for intelligence-collection and exchange and forensics at many different levels.

These different factors, all of which are currently owned or managed by different institutional stakeholders and to a greater or lesser degree work independently of each other, should work more collaboratively in concert. For example, threat intelligence will only be useful if it takes in data that Member States themselves do not possess. Training curricula need to be kept up-to-date, which will only be possible via technological know-how provided by the security industry and R&D functions.

8.1 Towards a pan-European cybercrime capability

In order to deliver successfully on these aspects outlined above, we propose that these developments, instead of being viewed in isolation, are instead taken into the context of a "pan-European cybercrime capability" with the ECC at its centre. This builds on our understanding of the coherent way in which the EU-level stakeholders must work together for the benefit of Member States, businesses and citizens. We suggest, and base our implementation plan on, the formulation of a Capability Board, which would be run by the ECC. This entity would help tie together the disparate interests of those stakeholders with responsibility for different elements of the European effort against cybercrime, as detailed above.

This capability-based approach has been delivered in a law enforcement setting[44] and is also common in complex public-sector initiatives that can last several years and involve significant expenditure.[45] The Capability Board, comprising a representative from each stakeholder with responsibility for delivering a particular part of a capability (e.g. training, for example), would convene annually to determine what is needed to ensure that capability is delivered in a timely manner. Thus the owner of each "Line of Development" (e.g. training, doctrine, personnel, etc.) is able to observe his peers' progress. The

[44] Personal communication Tim Barber, Director, KPMG Advisory 23/01/2012

[45] As of 15 February 2012: http://www.aof.mod.uk/

Chairman of the Capability Board (in this case the Head of the ECC) has the mandate to slow down or speed up the delivery of certain aspects in order to ensure that a capability and not simply isolated elements are provided as an output. Through dint of the ECC Head being the chair, he or she would be able to use the ECC as the steering organisation for the development of a pan-European capability to address cybercrime. Although he or she would not have control over budgets of participating organisations, as Head of the ECC the postholder would be accountable for the delivery of a capability to Europol's Management Board and EU-level institutions (e.g. the European Council and Parliament) and thus would have a stake in encouraging all participants to work collaboratively.

The participants on the proposed ECC Capability Board would include at a minimum, Europol, Eurojust, CEPOL, ENISA, the Chair of the EUCTF, the designated strategic Harmony cycle representative, a representative from the national/governmental CERT community and possibly the private sector. The Capability Board would not seek to undermine the work of the EUCTF, but rather provide top-down support for its deliberations. Some material would be necessarily restricted but the aim would be to promote sharing of information between all organisations that possess responsibility for specific parts of a pan-European capability to address cybercrime.

8.2 Model of approach

In order to provide for the greatest degree of flexibility, we base this implementation roadmap on a two-pronged approach:

- **Principles** are conclusions directly stemming from the evidence described above indicating those things which are seen as critical to the successful delivery of a capability to deal with serious and organised cybercrime.
- **Approaches** are possible routes to implementation that we have suggested below as being most feasible given the evidence base generated from this study and parallels indicated elsewhere in domains that share similar characteristics. These are based on available data provided to us or identified during the course of this work from sources such as those from the main EU institutions, Interpol, Member States, industry or other academic and research institutions.

8.3 Principles

8.3.1 The participation and contribution of Member States must be central to the efforts and impacts of the ECC

This is particularly the case with respect to the contribution of MS to the strategic intelligence picture, as the quality of this intelligence depends very much on information submitted by Member States. We recognise that information asymmetries that exist with respect to the sharing of intelligence are not necessarily unique to cyberspace. Other law enforcement and intelligence agencies also report that information asymmetry does not have a simple or elegant solution but requires constant effort (e.g. see Willis, *et al*, 2009). The implication of this for the ECC is that it should not try to duplicate or start from scratch, but should build on existing trust relationships that encourage information sharing. Better data from Member States (see below) can provide the evidence-base illustrating where there are gaps in the intelligence picture and also support better quality products from the ECC to Member States in order to strengthen the virtuous circle of others being encouraged to contribute.

8.3.2 The oversight and governance of the ECC must involve all key players, including non-law enforcement partners

This would encourage shared responsibility for cybercrime. Europol has complex oversight arrangements which are in accordance with the mandate of the agency as a criminal intelligence organisation. Europol's activities are currently overseen by committees of the Council (COSI) and by the European Parliament via the Europol Joint Supervisory Board (JSB). Given the challenges in securing the necessary co-operation and co-ordination in the field of cybercrime, findings from our study indicate that there could be benefits to some additional, specific governance arrangements for an ECC, which could act to help drive accountability for the delivery of a broad capability to address cybercrime. This governance mechanism would need to be in addition to existing governance arrangements for Europol and as described in Section 8.1 would manifest itself in the form of the ECC Capability Board.

8.3.3 The principle of subsidiarity must govern the scope of the ECC's work

Things that can be done best by Member States should be done by Member States. This extends to operational investigations in particular. Europol has no powers of arrest – it works on the basis of voluntary co-operation by Member States. Article 4(1) of the Europol Council Decision (European Council, 2009) states that Europol is to work in a reactive model. An ECC operating within the existing Europol governing framework should intervene only where there is a clear multinational (by which we mean pan-European or even international) rationale. These areas range from strategic intelligence to facilitating co-operation; exchanging best practice and keeping a watching brief on technology evolution to advise on, for example, crimeproofing.

The ECC should start small to enable early success. Initial activities should focus on meeting small, well bounded and achievable objectives related to the provision of help and support to Member States (who, as previously noted, are the main customer and contributor to the ECC). There are three reasons for advocating this principle of starting small. Firstly, focusing small (as OECD best practice on public sector initiatives indicates)[46] is a way to manage risks more effectively and ultimately ensure successful achievement of bigger objectives in the longer term. Secondly, the trust that characterises existing relationships between Europol and Member States has taken many years to develop. It would be naive to suggest that these can be replicated easily over the course of

[46] For a discussion of IT-enabled change in the public sector, see OECD Public Management Policy Brief (PUMA WP) No. 8 (2001)

the first year of the ECC. Thirdly, if the ECC were able to effect solutions to minor but well scoped problems quickly this would be highly effective in demonstrating the added value of the ECC.

8.3.4 The ECC should be flexible in focusing its resources depending on the type of cybercrime

This principle follows from the principle of subsidiarity, Europol's existing areas of competence as defined in the ECD (European Council, 2009) and its Article 4(1) mandate and Annexe of "Computer Crime" and the need to maximise the added value of a new European-level capability to deal with serious forms of cybercrime. The ECC should not attempt to duplicate MS-level efforts (commensurate with their own cultural, historical and criminal justice contexts) for example by dedicating pan-European intelligence and operational support resources to dealing with volume forms of "petty" cybercrime. The ECC should have as a starting point a principle that the use of its resources should be tailored to the type of crime. For example, intelligence resources should first be targeted in the main to what is termed by the Council of Europe as "crimes where information and data are the targets" in addition to focused areas of competence (specifically Internet-facilitated online child exploitation). This is not to say that the ECC would disregard other forms of cybercrime. For example, assuming a better information flow between the ECC and the national/governmental CERT community, the ECC should be able to target its expensive strategic intelligence resources to those incidents where volume crime, such as phishing, becomes so prevalent that the stability and integrity of the European financial system is put at risk. The ECC will indirectly support Member States in dealing with volume cybercrime and with offences by means of ICT and offences involving ICT, though the provision of training and sharing best practice.

8.3.5 The ECC must operate with respect for data protection and fundamental rights

This principle is central to all of Europol's work governing the use of sensitive personal data in its intelligence and operational support activities. Europol's existing data protection regime is widely considered to be mature (in the context of criminal justice activities), and is overseen by both the Data Protection Officer and the Joint Supervisory Board (JSB). The exiting regime is, however, complex and highly nuanced, requiring a deep understanding of the proportionality around the intrusion into the private sphere in order to achieve law enforcement and criminal justice goals.

8.3.6 Greater co-operation between law enforcement and CERTs will be crucial to the delivery of an improved cybercrime capability

CERTs sit at the front end of incident response. From the information reported to them from the business community they often have a detailed picture of incidents as they evolve and are reported. This means that CERTs hold information that could usefully feed into the development of both tactical and strategic intelligence by the ECC. However, there is evidence that CERTs are sometimes reluctant to share information with law enforcement. One reason for this is a difference in underlying aims and objectives: CERTs consider law enforcement to be primarily concerned with securing evidence (which may mean shutting down the system of a business that has been a victim of cybercrime, whereas CERTs are primarily concerned with supporting businesses in overcoming the problem and maintaining business functionality. Additionally, private-sector players often report reluctance to report to law enforcement because the police cannot respect anonymity of the source. Co-operation between the ECC and the CERT community must therefore be based on mutual understanding of competencies and operating principles from both law enforcement and the CERT community. However, due to the existence of many different types of CERT, as we have seen, we make explicit that national/governmental CERTs be selected as the primary vehicle for establishing deeper co-operation and strengthening information sharing between Member State level law enforcement capability, the CERT community more generally and the ECC.

This approach also yields other benefits related to strengthening capacity at Member State level. As reported in (ENISA, 2011), national / governmental CERTs exhibit uncertainty with regards to the sharing of information across borders, and procedures for dealing with law enforcement, the presence of an LEA would therefore also benefit peer to peer information exchange between national / governmental CERTs (and a pan European capability to address cybercrime). Although efforts are already underway, as we have seen in Chapter 5, to strengthen co-operation in the CERT community, supported by ENISA, we recognise that the ECC may play an important role in encouraging greater co-operation between law enforcement and CERTs at national level.

8.3.7 An ECC must build broad-based capability within Member States to deal with the many different types of cybercrime through training education and dissemination of best practice

There is plenty of scope to improve the ability of national criminal justice systems to deal with cybercrime. The aim is to encourage a view of cybercrime as pervasive, instead of as a specific type of crime with unique characteristics, in order to build on a strong criminal justice capability to address cybercrime at the local level. The institutionalisation of cybercrime capabilities will help ensure law enforcement efforts are better able to understand correlations between crimes across different domains.

Firstly, this can be achieved through training, and it will be important for an ECC to have a clear view of how it will work with CEPOL (and other groups such as ECTEG) to deliver both basic and advanced cybercrime training. Secondly, it could be achieved by broadening the customer base for training from just law enforcement to other criminal justice personnel. This is especially important with respect to the judiciary – both public prosecutors and judges. During fieldwork we heard that prosecutors and judiciary often have very low levels of understanding of cyber issues, and often do not have access to training and education in this field. Clearly, the ECC should work closely with Eurojust in refreshing or developing any training for prosecutors or the judiciary. The European added value of the ECC in this regard is certainly to be found in providing guidance, handbooks and disseminating best practice – for example on specific approaches to forensically read a particular disc drive or perhaps via sharing of software tools written specifically for unique and exotic devices.

8.3.8 An ECC must strengthen Europol's existing capability in intelligence analysis and operational support, based on a broader information picture

Our research found that most stakeholders were of the view that, largely, there were no structural deficiencies with respect to Europol's current activities. However, there was scope to develop this capability. For example, some participants in the study reported that information exchange was problematic due to a perception of slow response and turnaround procedures (particularly for the AWF mechanism) and the poor added value of the AWF model for some contributors.

At the same time, participants in the study reported that the dedication of more and more resources to cybercrime would possibly be an ultimately futile exercise: there was always "more than enough cybercrime to go around" This links to the implicit finding of Chapter 2 that the unreliability of current figures as to the extent of cybercrime makes them a poor basis for resource allocation. Instead, better information and intelligence is required to target resources in a more precise manner to determine where to apply capability on the basis of the severity of the impact to society the economy.

8.3.9 An ECC should support a common infrastructure for cybercrime reporting between law enforcement, members of the public and the private sector

With respect to online reporting and exchange of cybercrime reports, it is understood that, work is underway in Europol through the ICROS programme to develop a common platform for broad-based reporting. However, some of the feedback collected during our study from those Member States participating indicated that the resources dedicated to running online reporting platforms might also be usefully deployed elsewhere (in, for example, intelligence-gathering). Although online reporting platforms appear to have a role to play in the provision of tactical intelligence to aid investigations, at a strategic level it was seen that resources could be dedicated more effectively to other activities that would have a greater law enforcement contribution (e.g. covert surveillance). Furthermore, there are other strategic infrastructure considerations with respect to the collection of actual victimisation reports in an online form. Notably these revolve around the provision of identification documents by the victim. To be fully effective, a European-level reporting system with the aim of directly collecting victim reports online would thus require a pan-European-level mechanism to verify electronic identity credentials. There is also the question of fragmentation of reporting platforms both at national level and also between sectors. This is particularly the case with those reporting platforms confronting citizens. For example, recent industry data suggests that only a small percentage of the population reports an incident to law enforcement. This was also supported by the UK British Crime Survey (BCS) which included forms of cybercrime in its 2003–2004 victimisation survey but the inclusion of cybercrime as a category was discontinued, reportedly because of the low level of reports (Wall, 2011). Therefore, any efforts by the ECC to establish a mechanism for the direct reporting of victimisation reports would need to take care to avoid concerns relating to fragmentation and the utility of online victimisation reports.

8.3.10 Over the long term, the ECC should work to develop an improved common picture of the extent of cybercrime

This should be achieved by leveraging data from a number of sources; not least those in the national/governmental CERT community, as well as from other open sources. Although the option seen as most feasible reflects the importance of Europol as a source of intelligence (since via the AWF infrastructure it has better understanding of sensitive criminal intelligence to which others may not be privy), it is important to note that with respect to cybercrime the private sector plays an important role in providing information. Better data on the extent of the problem may have the following benefits:

- If Member States were to receive intelligence products based on more extensive data (that they themselves could not afford) coming from the ECC then they might be more incentivised to contribute (especially to the AWF structure).
- If industry were to get better quality data on evolving *modus operandi* of cybercriminals via the ECC then it might have the effect of encouraging information exchange, since it would go some way to showing that over time each player in a specific sector suffers equally. Although it is widely understood that the distribution of attacks is not normal, over time, by better quality data, it may be possible to show at sector level that every firm will be affected at some point.
- More efficient allocation of law enforcement resources both at European and national level.

8.4 Roadmap

We now turn to a proposed practical implementation timeline for the activities set out in Chapter 7 according to the principles laid out above. This sets out how the activities should be undertaken and in what order, in order to achieve first Initial Operating Capacity (IOC) and then Full Operating Capacity (FOC).

8.4.1 "Pathfinder phase" to Initial Operating Capability (IOC) – June 2012 to December 2013

In Year 1 of the ECC (2013) we propose that the following activities are undertaken in order to achieve IOC in line with the programme-based approach described earlier. We term this the "pathfinder phase". These activities revolve around governance arrangements and beginning work streams to allow the activities of the ECC, described above, to be effective. Broadly, each of these activities incurs an additional resource implication aside from the activities relating to "Sensitive Criminal Intelligence Analysis and Investigative Operational Support" which, for this pathfinder phase, Europol would conduct according to the current status quo, until more information was available from the LEA–CERT PPP Network.

We describe these activities along the headlines of:

- Governance.
- Criminal intelligence and operational support.
- Broad-based training, education and good practice sharing.
- Data fusion, and collaborative working with the national/governmental CERT community via a Joint LEA–CERT Network and the ECRF for the broader criminal justice community.
- Facilitating a reporting platform of use to law enforcement, members of the public and the private sector.

Governance

The Head of the ECC, Project Manager and Administrative Support posts are formulated, created and filled to staff the ECC governance team. The activities that this team would perform would be to:

- Prepare co-operation agreements (to cover the Liaison Officer roles).
- Organise administrative and governance matters (e.g. the organisational structure to bring together existing capabilities under the administrative roof of the ECC).
- Conduct planning for the co-operation and co-ordination cell of the ECC.
- Work to prepare the first meeting of an ECC Capability Board, which will set the agenda for a pan-European cybercrime capability, with the ECC at its heart.

The ECC governance team would be required to prepare the agenda for the Capability Board and its first meeting.

In addition, the cross-border nature of this domain requires the creation of links with other activities, particularly those of Interpol and other third countries. This could be based on the existing Strategic Co-operation Agreements currently developed by Europol as a starting point.

In addition to facilitating the work of the ECC Capability Board, the ECC governance team would also act as a support to the EUCTF, an important platform for Member States. The ECC governance team would thus be able to support the background work of the EUCTF at the direction of the Chair and Vice Chair.

Other preparatory exercises would include conducting a readiness exercise to assess the readiness of each stakeholder (Europol Eurojust, CEPOL and ENISA) to participate in the ECC Capability Board and identify any gaps or weaknesses requiring specific attention.

Funding channels should be identified and established to allow resources to flow from the ECC to Member States to support the establishment of law enforcement personnel to be physically co-located with national/governmental CERTs. Without recreating the existing

ENU infrastructure, these focal points would be responsible for completing an intelligence requirement to be fed to the ECC (probably via the ENUs). This funding stream should be based on the model of the European Centre for Monitoring of Drugs and Drug Addiction (ECMDDA) which, via its Reitox Network is faced with similar challenges in the different domain of illicit drugs. It is proposed that using this model a contribution is made from the budget allocated to Europol to establish the ECC to the set-up of CERT Liaison Officers, subject to the unique characteristics of Member States, to physically be co-located alongside technical staff in the national/governmental CERTs.

Given the similarities of equipment across Member States the ECC governance team could consider other relatively easy goals such as the creation of a catalogue of hardware, software and training products and services. This would gather common requirements from Member States and allow negotiation with the manufacturers and providers of such software and hardware tools in order to achieve better prices. This would demonstrate clear added value to the Member States through offering them the possibility to obtain commonly used tools at a better price.

Further fact-finding research would be necessary, for example, to collect and catalogue definitively how each Member State approaches information-sharing, to provide the LEA–CERT Network members with a handbook to help them break down barriers of misunderstanding between these two types of organisation.

Criminal intelligence and operational support

The IOC would see existing criminal intelligence and operational support measures continue under the current resource level, until such time as a better flow of higher quality information from the Joint LEA–CERT Network would allow a more informed allocation of resources to these activities.

Broad-based training, education and good practice sharing

Additional resources should be made available to extend basic cybercrime training to those from judicial authorities across the EU Member States. Recognising the important role of CEPOL in acting as conduit to build a broad-based capability (via its links to national police colleges) and the role of ECTEG in developing course content (albeit aimed at individual customers) we propose that in the first year, training, education and good practice development be strengthened and enhanced. We base training provision on a model of continuous professional development. This would take the form of five-day courses (based on the current training arrangements from Europol which are structured around five-day courses) with funding made available through the ECC to cover the costs of attendance.

In addition, information seminars and best practice development (the collection, creation and dissemination of accessible operational level guidance to Member States) would also take place.

Co-operation and co-ordination

For the pilot phase we propose that additional resources be used to set up the information exchange mechanisms between the ECC and MS-level national/governmental CERT community and a ECRF to strengthen further the non-law enforcement capabilities of the criminal justice system. We detail each of these below.

Joint LEA–CERT PPP Network and ECC Data Fusion Unit

We suggest a staged approach to implementing the LEA–CERT information exchange activities of the ECC as detailed in Chapter 7. This involves two closely linked areas. We assume a relationship between establishing a more accurate picture of overall cybercrime phenomena (possible through more extensive multi-source intelligence gathering) and the aforementioned deployment of operational support resources and criminal intelligence analysis to more comprehensively understand and thus manage cybercrime.

The implication of this is that until mechanisms are in place to gain better insight into cybercrime, caution should be exercised in appropriating and deploying additional criminal intelligence resources as within Europol's own Operations Department. Therefore, in the pathfinder phase, we propose that a pilot of the Joint LEA–CERT PPP Network is implemented as part of IOC, in order to test the validity of this model.

In line with the evolutionary "start small" principle outlined above, we suggest three countries are selected to be the candidates for this pilot exercise. We propose that candidates are countries where there are no existing mechanisms for public–private co-operation between CERTs and law enforcement. We further suggest that those countries are identified from a range of relevant criteria including numbers of citizens online.

The Joint LEA–CERT PPP Network would see joint working mechanisms between law enforcement personnel and the designated national/governmental CERT.

The Joint LEA–CERT PPP Network present in three pilot countries would thus feed data into the DFU (which as described would consist of a single post). This pilot would last for one year to test the working relationship of this model and information flow between the national/governmental CERTs; the ECC and Europol National Units.

We envisage that the information from this pilot would serve to inform any necessary changes to the current complement of criminal intelligence analysts required for Full Operating Capability.

To guide the work of these personnel, with the input of the European Union Cybercrime Task Force (EUCTF), the ECC governance team would prepare the aforementioned operational handbook describing for each MS under what conditions (existing in law and also operationally) they could usefully report information. In order to address the problem of guarantees of anonymity between the private sector and law enforcement it may be necessary to establish codes of conduct that guarantee anonymity. However, for this to work the judiciary must be brought in, which is why the training aspects are important since the chain of anonymity needs to be respected all the way through – from the police giving anonymity guarantees to the CERTs to the public prosecutor (who then, as currently indicated, might breach this). The code of conduct thus needs to be viable across three different types of stakeholder (law enforcement, judicial authority and national/governmental CERT) or at least involve all who are present in the chain of anonymity. Another option might be to use "hypothetical" case studies as reported to us by the BKA in Germany. The ECC could, for example, prepare a list of common hypothetical case studies that law enforcement or the private sector could use.

In addition, the implementation team should quickly establish links into the European Information Sharing and Alert System (EISAS).[47]

European Cybercrime Resource Facility

We also propose that in the pathfinder phase, three people are recruited to establish the ECRF (as detailed in Chapter 7). Again due to the sensitivity of these posts, we envisage these being recruited at full EU level. Given the reported need to improve and engage the broader criminal justice community (including public prosecutors and judges) by furthering their awareness and disseminating good practice concerning addressing cybercrime, the ECRF could be implemented relatively quickly to realise rapid benefits.

Facilitating broad online victim/witness reporting to a range of interested parties

The European Cybercrime Task Force (EUCTF) supported by the ECC governance team should lead a mapping exercise with respect to online reporting systems as a first step towards creating an interoperable standards-based application, using the previously identified IETF model (IODEF) as the basis. The output of this exercise would be to establish an interoperability map identifying a taxonomy or list of common terms and interpretations between those online reporting systems in existence in Member States. For example, some countries may collect [name] by an open text field and others may collect [firstname] and [lastname]. This taxonomy would permit greater understanding of what is meant by each field in use in each national reporting system and would be a necessary precondition to developing a standards-based online reporting tool.

Resource implication for "pathfinder phase"

Table 8.1 below indicates the overall additional staff (expressed in numbers of additional posts, over and above those currently active) for the ECC "pathfinder phase" to IOC.

Table 8.1 Additional personnel implication for "pathfinder phase" activities (Jan–Dec 2013)

Functional posts	Administrative Posts
5	2

Table 8.2 below indicates the additional resource implication for the pathfinder phase between January and December 2013. They include some, but not all, costs detailed earlier (for example they exclude the one-off costs of buying desktop IT equipment for any additional criminal intelligence analysis personnel and of course exclude further increases in resources to cover additional in criminal intelligence analysis and operational support personnel). These costs are detailed at Appendix F.

[47] ENISA, EISAS Feasibility Report (2007)

Table 8.2 Additional resource implication (€) for "pathfinder phase" activities (Jan–Dec 2013)

Item	Estimate (€)
One-off costs	600,000
Labour costs	1,000,000
Other ongoing expenditure	1,900,000
Risk and contingency	170,000
Total expenditure 'pathfinder phase' (Jan–Dec 2013)	3,670,000

We would suggest that at the conclusion of IOC in December 2013 further detailed planning and an evaluation will be necessary in order to confirm further financial implications going out to FOC. This evaluation should take account of the progress of the setting up training and professional development activities and in particular the success of the Joint CERT-LEA PPP model in those three countries selected to participate in a pilot. Further consideration and analysis of likely resources will no doubt be required especially given the rapidly evolving economic context. The evaluation would specifically need to critically collect and analyse information on cases and in addition quantitative and qualitative data of the Joint LEA-CERT PPP Network.

8.4.2 Towards Full Operating Capability (FOC) – Jan 2014 and beyond

After these initial measures are in place, we suggest that it may be possible to resource more precisely other areas as indicated, given the improved operational picture that it is hoped might emerge from the analysis of multi-source data.

- **Governance activities** would build on those conducted in IOC and also work on the development of a proposed evaluation and monitoring framework to link inputs (budgets, numbers of analysts) to throughputs (activities) to outputs (numbers of cases; number of intelligence reports; number of records) outcomes (numbers of criminals arrested; length of convictions) and impacts (measurable reduction in criminality; reduction in values of frauds per case).
- **The estimation of the resourcing needs**, between the modelled bounds of the low/high workload requirement for criminal intelligence analysis and operational support would now be informed by a much more precise and broader picture of the phenomena allowing the resource allocation for personnel to support these activities to fall between the following ranges:
    - **Low** workload requirement – an additional **21 personnel** (14 functional posts and seven support posts) to the reported June 2011 complement of Europol personnel working in this area.
    - **High** workload requirement – an additional **240 personnel** (158 functional posts and 82 support posts) to reported June 2011 complement of Europol personnel working in this area.

- **Training and education activities** would be more closely linked to the evolving nature of the phenomena
- **Co-operation and co-ordination activities** would be expanded thus:
  - The Data Fusion Unit would expand from the single post allocated to participate in the pilot by a further **four**, bringing the total to five, to cover the entirety of the EU (in line with the EMCDDA model).

Table 8.3 below indicates this scaling.

Table 8.3 Evolution of staffing of the proposed Data Fusion Unit

Phase	Additional posts	Total posts	Description	Total ongoing resources p.a. (€)
FOC (2014 onwards)	4	5	To receive data from EU-wide CERT Liaison Officers as per FOC in addition to private sector, APWG and trend analysis from MS running the standards-based reporting application	650,000

- **The LEA–CERT PPP Network would expand** to all countries having a designated national/governmental CERT requiring just under **€1.3 million** of funding (to cover a contribution of 75 percent from the ECC to assign to LEA–CERT PPP Network members). The other resource implications would be as already described in Chapter 7 based on the low/high workload requirement.

Personnel resource summary

We present the growth of personnel over time for the low/high workload requirement in Table 8.4.

Table 8.4 Summary of growth in resources under the low workload requirement

Activity	New personnel pathfinder phase (2013)	New personnel (2014)	Total ongoing personnel thereafter
ECC governance team	3	0	3
Criminal intelligence and operational investigative support	0	21	21
Data Fusion Unit	1	4	5
European Cybercrime Resource Facility	3	0	3
Total	**7**	**25**	**32**

Table 8.5 Summary of growth in resources under the high workload requirement

Activity	New personnel pathfinder phase (2013)	New personnel 2014	Total ongoing personnel thereafter
ECC governance team	3	0	3
Criminal intelligence and operational investigative support	0	240	240
Data Fusion Unit	1	4	5
European Cybercrime Resource Facility	3	0	3
Total	**7**	**244**	**251**

Table 8.6 below restates the overall budgetary implication provided in Section 7.7 on resources. It is important to note again that one-off costs are represented both in Section 7.7 under non-labour costs but also here.

Table 8.6 Summary of expected one off capital expenditure resource implication for preferred option in 2014 (€m)

Option	Total Resources (€m)	
	Low workload requirement	High workload requirement
One-off costs	0.15	1.0

Note that in 2014 there will be additional capital expenditure required to purchase ICT infrastructure for additional personnel to perform tasks relating to criminal intelligence analysis and operational support and the Data Fusion Unit (DFU). We thus present the table below which includes these additional one off capital expenditures for 2014 only.

Table 8.7 Summary of expected total resource implication in 2014 (€m)

Option	Total resources (€m)	
	Low workload requirement	High workload requirement
One-off costs	0.15	1.0
Total ongoing costs	7.35	41.3
Risk and contingency	0.36	2.1
Total programme costs	**7.72**	**44.4**

Table 8.8 below shows the resource estimate for operational expenditure on an ongoing basis for the years after 2014. However, we would expect that, as with the period from IOC to FOC, a more formal budgetary review would take place in order to assess the continued validity of these estimates.

Table 8.8 Summary of estimated ongoing resources (p.a.) for preferred option for subsequent years (€m)

Item	Total resources (€m)	
	Low workload requirement	**High workload requirement**
Ongoing labour costs	4.3	32.9
Ongoing non-labour costs	3.05	8.8
Total ongoing costs	7.35	41.3
Risk and contingency	0.36	2.1
Total ongoing costs	**7.71**	**43.4**

8.5 Conclusion

This final chapter of the Feasibility Study has described how the ECC might be set up, building from a number of principles. It is important to recognise two main structural considerations – firstly, that the current climate of austerity weights heavily against new expensive initiatives (such as the creation of a brand new physical building to house an ECC) and, secondly, that without a broader information picture, it would be ineffectual to deploy further the resources of Europol analysts. We also note the importance of adopting a broad-based capability approach to addressing cybercrime, with the ECC at its heart, which would bring together existing efforts from some of the public and private organisations we have considered. The principles for the implementation of the ECC include the following:

- The participation of Member States must be central to the efforts and impact of the ECC.
- The oversight and governance of the ECC must involve all key players including non-law enforcement partners.
- The principle of subsidiarity must govern the scope of the ECC's work.
- The ECC should be flexible in focusing its resources depending on the type of cybercrime.
- The ECC must operate with respect for data protection and fundamental human rights.

- Greater co-operation between law enforcement and the national/governmental CERT community will be crucial to the delivery of an improved cybercrime capability.
- The ECC must support a broad based capability within Member States.
- The ECC must strengthen Europol's existing capability based on a broader information picture.
- The ECC should set up a common infrastructure for reporting and exchange of cybercrime relevant data between many different types of interested parties.
- Over the long term, the ECC should work to develop an improved common picture of the extent of the phenomena of cybercrime.

To achieve these high-level principles we propose a two-stage implementation with a small pathfinder phase in 2013, leading to Full Operating Capability in 2014. In particular, the initial phases would put in place measures to inform more effective deployment of Europol's valuable sensitive criminal intelligence and operational support measures.

As has been shown, there exists great complexity in the phenomena of cybercrime, with multitude of actors and organisations each playing their role and being responsible for different elements that need to be brought together seamlessly in order to address cybercrime successfully. The challenges to setting up the ECC include the differing institutional character of each stakeholder organisation, the complexity of their perspectives and understanding the way in which each activity may be dependent upon another and the need to involve non-law enforcement stakeholders who may be motivated differently – and the interconnectedness and interdependency of each activity. Finally there is the acceptability of establishing wholly new organisational structures, especially in the current economic climate.

In the provided roadmap, the benefits of bringing these different parts together include:

- Better understanding of the phenomenon derived from strategic analysis utilising a broader range of sources.
- Support for side-by-side working between law enforcement and the national/government CERT community, which would also support the strengthening of cross-border information exchange between CERTs.
- More systematic provision for the sharing and exchange of knowledge between all members of the criminal justice community.
- A stronger basis for support of training and professional development, permitting a more sustainable pan-European capability against cybercrimes which may involve computers or where technology plays a role but is not necessarily the target.
- A systematic means, consistent with state-of-the-art developments in the private sector to provide a common, standards-based platform to report and exchange strategically useful data on cybercrime between and amongst law enforcement, the private sector and citizens.

The ECC will need to take a foremost role in pushing the enhancement and growth of a broad and systematic capability to address cybercrime. The ECC appears to fulfil a gap in providing a facility that can enhance knowledge, build capability and improve security in the face of cybercrime.

This report has aimed to shed some light on the complexity, the needs, the options and the likely risks and costs associated with different options to establishing the ECC Finally, we have sought to provide a possible route through the complexity with the establishment of an ECC according to a suggested approach and timeline.

REFERENCE LIST

List of references

Aldesco, A. I. (2002). "The demise of anonymity: a constitutional challenge to the convention on cybercrime", *Entertainment Law Review,* 23(1), pp. 81–123

Alkaabi, A., G. M. Mohay, A. J. McCullagh and A. N. Chantler (2010). "Dealing with the problem of cybercrime", Conference Proceedings of 2nd International ICST Conference on Digital Forensics & Cyber Crime, 4–6 October 2010, Abu Dhabi. As of 17 February 2012: http://eprints.qut.edu.au/38894/1/c38894.pdf

Anderson, R. (2001). Why information security is hard - an economic perspective. *Computer Security Applications Conference, 2001*. ACSAC 2001. Proceedings 17th Annual Computer Security Applications Conference.

Anderson, R., R. Bohme, R. Clayton and T. Moore (2008). "Security economics and the internal market." As of 17 February 2012: http://www.enisa.europa.eu/act/sr/reports/econ-sec/economics-sec/at_download/fullReport

Anderson, C. L. and R. Agarwal (2010). "Practicing safe computing: a multimethod empircal examination of home computer user security behavioral intentions." MIS Quarterly 34(3): 613-643.

ANSSI (Agence nationale de la sécurité des systèmes d'information) (2011), «Défense et sécurité des systèmes d'information: stratégie de la France». As of 13 February 2012: http://www.ssi.gouv.fr/IMG/pdf/2011-02-15_Defense_et_securite_des_systemes_d_information_strategie_de_la_France.pdf

ASEAN Regional Forum (2010). Co-chairs Summary Report of the ASEAN Regional Forum Cybercrime Capacity Building Conference held in Bandar Seri Begawan, Brunei Darussalam, April 27–28 2010". As of 15 February 2012: http://aseanregionalforum.asean.org/library/arf-chairmans-statements-and-reports.html

Association of Chief Police Officers of England (2009). ACPO e-crime Strategy 2009 Report,

Baker, W., A. Hutton, C. D. Hylender, J. Pamula, C. Porter, and M. Spitler (2011). 2011 Data Breach: Investigations Report, A study conducted by the Verizon RISK Team with co-operation from the U.S. Secret Service and the Dutch High-Tech Crime Unit. As of 17 February 2012:

http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf

BBC (2011). "London hosts cyberspace security conference." from http://www.bbc.co.uk/news/technology-15533786.

Beker, S., N. Filipiak and K. Timlin (2010). "In the dark: crucial industries confront cyberattacks", McAfee Second Annual Critical Infrastructure Protection Report, written with the Center for Strategic and International Studies (CSIS). As of 17 February 2012: http://www.mcafee.com/us/resources/reports/rp-critical-infrastructure-protection.pdf

Blanco-Hache, A. C. and N. Ryder (2011). "'Tis the season to (be jolly?) wise-up to online fraudsters. Criminals on the Web lurking to scam shoppers this Christmas: a critical analysis of the United Kingdom's legislative provisions and policies to tackle online fraud", *Information & Communications Technology Law,* 20(1), pp. 35–56

Bourke, M. L. H. A. E. (2009). "The Butner Study redux: a report of the incidence of hands-on victimisation by child pornography offenders", *Journal of Family Violence,* 24, pp. 183–191

Brenner, S. (2002). "Organized cybercrime? How cyberspace may affect the structure of criminal relationships", *North Carolina Journal of Law and Technology,* 4, pp. 1–50

Brown, D. C. G. and G. Kourakos (2003). *Public Policy Forum RoundTable on Identity Theft and Identity Fraud.* Unpublished manuscript, Ottawa.

Bundeskriminalamt, R. O. (2011). "Crime trends in Austria in 2011: decrease in burglary and car theft; increase in violent crime and cybercrime." Vienna: Bundesministerium für Inneres.

Bundestag (14/8/2009). Act to Strengthen the Security of Federal Information Technology". As of 13 February 2012: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/BSI/BSI_Act_BSIG.pdf?__blob=publicationFile

Caballero, J., C. Grier, C. Kreibich and V. Paxson (2011). "Measuring pay-per-install: the commoditization of malware distribution", Proceeds of the USENIX Security Symposium, August 2011. As of 15 February 2012: http://www.icir.org/vern/papers/ppi-usesec11.pdf

Cabinet Office (2009). Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space, (Cm 7642). As of 17 February 2012: http://www.official-documents.gov.uk/document/cm76/7642/7642.pdf

Cain, P. and D. Jevans (2010). Request for Comments 5901. As of 16 February 2012: http://www.ietf.org/rfc/rfc5901.txt

Canadian Bankers' Association (2003). "Identity theft: An old problem needing a new approach."

Centre for Strategy and Evaluation Services (2007). Final Report: External Evaluation of the European Monitoring Centre for Drugs and Drug Addiction", European Commission, 2007. As of 16 February 2012: http://www.emcdda.europa.eu/attachements.cfm/att_46509_EN_EMCDDA Evaluation - Main Report (12.12.07) PDF.pdf

Commonwealth Australia (2010). "Hackers, fraudsters and botnets: tackling the problem of cyber crime", Report of the Inquiry into Cyber Crime, Canberra: House of Representatives: Standing Committee on Communications

Congressional Record (1998). Sec. 7 Reaction of Ethics Reports Filed by Judicial Offices and Employees. *V 144*. As of 17 February 2012: http://books.google.com/books?id=m5wLgC546hMC&pg=PA24381&lpg=PA24381&dq=credit+card+fraud+$400+million+annually&source=bl&ots=XX7MV_0jDZ&sig=uOK_4w3LqbBhxtkIBQeKNeg7y8I&hl=en&ei=cvGvTv7OBYnFtgesmqWuDQ&sa=X&oi=book_result&ct=result&resnum=1&ved=0CBwQ6AEwADgK#v=onepage&q=credit%20card%20fraud%20%24400%20million%20annually&f=false

Council of the European Union (2005). Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems. Official Journal L 069 , 16/03/2005 pp. 0067–0071. As of 15 February 2012: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32005F0222:EN:HTML

Council of the European Union (2008). Council Conclusions on setting up national alert platforms and a European alert platform for reporting offences noted on the Internet, 2899th Justice and Home Affairs Council meeting Luxembourg, 24 October 2008. As of 15 February 2012 http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/jha/103537.pdf

Council of the European Union (2008). Council Conclusions on a Concerted Work Strategy and Practial Measures Against Cybercrime, 2987th Justice and Home Affairs Council meeting Brussels, 27–28 November 2008. As of 15 February 2012: http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/jha/104344.pdf

Council of the European Union (2009). EC Decision of 6 April 2009 establishing the European Police Office (Europol) (2009/371/JHA)). As of 17 February 2012: https://www.europol.europa.eu/sites/default/files/council_decision.pdf

Council of Europe (2010). Octopus Programme 2010. As of 15 February 2012: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy-activity-interface-2010/presentations/Ws 1/Nicola Di Leone_ECTEG.pdf

Council of Europe (2011). Convention on Cybercrime Status, CETS No: 185. As of 17 February 2012: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG

Cross, M. (2008). *Scene of Cybercrime*, New York: Syngress Elsevier

Cuganesan, S. and D. Lacey (2003). "Identity Fraud in Australia: An evaluation of its nature, cost and extent", Sydney: Standards Australia International Ltd

Dunn, M. and I. Abele-Wigert (2006). The International Critical Information Infrastructure Protection (CIIP) Handbook. Bern, Centre for Security Studies, Swiss Federal Institute of Technology.

Deflem, M. and J. E. Shutt (2006). "Law enforcement and computer security threats and measures", in H. Bidgoli (ed.), *The Handbook of Information Security Vol.2*. NJ: John Wiley & Sons.

Detica (2011). "The Cost of Cybercrime", A Detica report in partnership with the Office of Cyber Security and Information Assurance in the Cabinet Office (UK). As of 17 February 2012:. http://www.baesystemsdetica.com/resources/the-cost-of-cyber-crime/

EECTF (2011). 2011 EECTF European Cybercrime Survey. As of 17 February 2012: http://www.poste.it/salastampa/CYBER_CRIME.pdf

Ehuan, A. (2010). "Chapter 10: Cybercrime and law enforcement co-operation", in J. Bayuk (ed.), *CyberForensics: Understanding Information Security Investigations*, London: Springer, pp. 129–140

ENISA (2007). EISAS Feasibility Report 2006/2007. As of 16 February 2012: http://www.enisa.europa.eu/act/cert/other-work/eisas_folder/EISAS_finalreport.pdf

ENISA (2010). "Baseline capabilitites for national/governmental CERTs". As of 15 February 2012: http://www.enisa.europa.eu/act/cert/support/baseline-capabilities

ENISA (2011a). "A flair for sharing – encouraging information exchange between CERTs". As of 15 February 2012: http://www.enisa.europa.eu/act/cert/support/legal-information-sharing

ENISA (2011b) "Resilience of the Internet Interconnection Ecosystem" April 2011 As of 19th Febuary 2012: http://www.enisa.europa.eu/act/res/other-areas/inter-x/report/interx-report

ENISA (2011c) 'Technical Guidelines on Implementing Minimum Security Measures: Guidance on the security measures in Article 13a Version 1.0, December 2011

ESET Threat Blog (2011). Retrieved 10 November 2011. As of 17 February 2012: http://blog.eset.com/2011/10/12/mining-social-data-led-to-johansson-and-aguilera-hacks

European Commission (2006). Proposal for a Council Decision establishing the European Police Office (EUROPOL) COM(2006) 817 final [Not published in the Official Journal]. As of 15 February 2012: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0817:FIN:EN:PDF

European Commission (2008). Report from the Commission to the Council based on Article 12 of the Council Framework Decision of 24 February 2005 on attacks against information systems, COM (2008)448. As of 15 February 2012: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0448:FIN:EN:PDF

European Commission (2010). Communication from the Commission to the European Parliament and the Council. The EU Internal Security Strategy in Action: Five steps towards a more secure Europe. COM(2010) 673 final. As of 15 February 2012: http://ec.europa.eu/commission_2010-2014/malmstrom/archive/internal_security_strategy_in_action_en.pdf

European Committee for Stanardisation (2008) CEN Workshop on 'Coding of Information and Traceability of Human Tissues and Cells' - WS/Tissues and cells - Closed Annex 4: Survey of systems characteristics, As of 12 Febuary 2012 http://www.cen.eu/cen/Sectors/Sectors/ISSS/Activity/Pages/Tissues_and_cells.aspx

European Financial Coalition against Commercial Sexual Exploitation of Children Online (2010). "14 months on: A combined report from the European Financial Coaltion: An intelligence assessment on the commercial distribution of child sexual abuse images – a progress report on the work of the European Financial Coaltion". as of 17 February 2012: http://www.ceop.police.uk/Documents/EFC%20Strat%20Asses2010_080910b%20FINAL.pdf

European Union (2010). The Stockholm Programme – An open an secure Europe serving and protecting citizens. Official Journal C115, 04/05/2010, pp. 001–038. As of 15 February 2012: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:115:0001:01:EN:HTML

Europol (2011a). *The European Investigator*. As of 15 February 2012: https://www.europol.europa.eu/sites/default/files/publications/investigator.pdf

Europol (2011b). Europol Work Programme 2012, EDOC #516774v25, 25th August 2011. As of 15 February 2012: http://register.consilium.europa.eu/pdf/en/11/st13/st13516.en11.pdf

Europol (2011c). Final Budget and Staff Establishment Plan 2011 (extract of file no. 2210–281). As of 15 February 2012: https://www.europol.europa.eu/sites/default/files/budget2011.pdf

Europol (2011d) ICROS Status Report 2nd December 2011

Europol (2011e). Summary for RAND Europe and DG HOME of Europol Costing Exercises for the European Cybercrime Centre (ECC), File no. 2720-29, The Hague, 20 October 2011

Europol (2011f). Threat Assessment (abridged) – Internet-facilitated organised crime – iOCTA. As of 17 February 2012: https://www.europol.europa.eu/sites/default/files/publications/iocta.pdf

EU Services (2008). Note de l'unite BUDG/A5 du 15/09/2008 ref MM D(2008)58297. Note à l'attention des Chefs d'unites responsables de ressources humaines et/ou financiers Bruxelles le 13 octobre 2008

Federation of Small Businesses (2009). "Online crime and fraud costs small businesses £800 each year, says FSB". As of 17 February 2012: http://www.fsb.org.uk/news.aspx?REC=5038&re=policy/news.asp

Ferwerda, J., N. Choucri and S. Madnick (2010). "Institutional foundations for cyber security: current responses and new challenges", Working Paper CISL# 2009-03, Cambridge, MA: Composite Information Systems Laboratory (CISL), Massachusetts Institute of Technology. As of 17 February 2012: http://web.mit.edu/ecir/pdf/madnick-2010-03.pdf

Florêncio, D. and C. Herley (2011). "Sex, Lies and Cybercrime Surveys", Microsoft Research. As of 17 February: http://research.microsoft.com/pubs/149886/SexliesandCybercrimeSurveys.pdf

Garlik (2009). UK Cybercrime Report, September 2009. As of 17 February 2012: http://www.garlik.com/file/cybercrime_report_attachement

Giles, J. (2010). "Spam, spam and more spam", *New Sci*entist, Vol. 205, No. 2749, pp. 44–45

Gordon, L. A. and M. P. Loeb (2006). "Budgeting process for information security expenditures." Communications of the ACM 49(1): 121-125.

Guinchard, A. (2011) "Between hype and understatement: reassessing cyber risks as a security strategy", *Journal of Strategic Secuirty,* 4(2), pp. 75–96

Hartel, P., M. Junger and R. Wieringa (2010). "Cyber-crime science = Crime Science + Information Security", Enschede: Centre for Telematics and Information Technology, University of Twente

Home Office (2005)."Fraud and technology crimes: findings from the 2002/03 British Crime Survey and 2003 Offending, Crime and Justice Survey", Home Office Online Report 34/05. As of 15 February 2012: http://webarchive.nationalarchives.gov.uk/20110218135832/http://rds.homeoffice.gov.uk/rds/pdfs05/rdsolr3405.pdf

Home Office (2006). New Estimate of Cost of Identity Fraud to the UK Economy. As of 19 February 2012: http://www.identitytheft.org.uk/cms/assets/cost_of_identity_fraud_to_the_uk_economy_2006-07.pdf

Home Office (2011). "New strategy to tackle cybercrime published". As of 17 February 2012: http://www.homeoffice.gov.uk/media-centre/news/cyber-strategy

House of Lords (2007). "Personal Internet security", House of Lords Science and Technology Committee, 5th Report of Session 2006–07 (HL Paper 165). As of 15 February 2012: http://www.publications.parliament.uk/pa/ld200607/ldselect/ldsctech/165/16502.htm

House of Lords (2008). "Personal Internet security: follow-up", House of Lords Science and Technology Committee, 4 th Report of Session 2007–2008 (HL Paper 131). As of 17 February 2012: http://www.publications.parliament.uk/pa/ld200708/ldselect/ldsctech/131/131.pdf

House of Lords European Union Committee (2010). "Protecting Europe against large-scale cyber-attacks" (HL Paper 68). As of 17 February 2012: http://www.publications.parliament.uk/pa/ld200910/ldselect/ldeucom/68/68.pdf

Hunt, P., B. Kilmer and J. Rubin (2011). *Development of a European Crime Report*, Santa Monica, CA: RAND Corporation.

IC3 (2010). IC3 2009 Annual Report on Internet Crime. As of 17 February 2012: http://www.ic3.gov/media/2010/100312.aspx

IC3 (2011). 2010 Internet Crime Report. As of 17 February 2012: http://www.ic3.gov/media/annualreport/2010_IC3Report.pdf

Ilett, D. (2006). "US to force firms to 'fess up on data loss” Security Strategy, silicon.com. As of 17 February 2012: http://software.silicon.com/security/0,39024655,39157787,00.htm

Internet Watch Foundation (2010). Annual and Charity Report. As of 17 February 2012: http://www.iwf.org.uk/assets/media/annual-reports/Internet%20Watch%20Foundation%20Annual%20Report%202010%20web.pdf

ITU (2008). Study on the Financial Aspects of Network Security: Malware and Spam. As of 17 February 2012: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-study-financial-aspects-of-malware-and-spam.pdf

Jamieson, R., L. Land, G. Stephens and D. Winchester (2008). "Identity crime: the need for an appropriate government strategy", *Forum on Public Policy/A Journal of the Oxford Round Table*, March 2008

Jenkins, J. (2011). "Man trolled the web for girls: cops", *The Toronto Sun* and Canoe.ca, retrieved 10 November 2011. As of 17 February 2012: http://cnews.canoe.ca/CNEWS/Crime/2007/12/07/4712680-sun.html

Keizer (2011). Zero-day bugs over-rated, Microsoft says. *Computerworld*, Computerworld.

Klimburg, A. and H. Tirmaa-Klaar (2011). "Cybersecurity and cyberpower: concepts, conditions and capabilities for co-operation for action within the EU". As of 17 February 2012: http://www.europarl.europa.eu/activities/committees/studies/download.do?language=en&file=41648

Ko, M. and C. Dorantes (2006). "The impact of information security breaches on financial performance of the breached firms: an empirical investigation." *Journal of Information Technology Management* XVII(2): 12-22.

Lemieux, F. (2011). "Investigating cyber security threats: exploring national security and law enforcement perspectives", Washington, DC: The George Washington University

Lovet, G. (2009). *Fighting cybercrime: Technical, juridical and ethical challenges*. Paper presented at the Virus Bulletin Conference, 23–25 September.

McAfee (2009). "Unsecured economies: protecting vital information. The first global study highlighting the vulnerability of the world's intellectual property and sensitive information". As of 17 February 2012: http://www.mcafee.com/us/resources/reports/rp-unsecured-economies-report.pdf

MessageLabs Intelligence (2007). 2007 Annual Security Report.

Mills, E. (2011). "Facebook bug-hunting scheme pays out $40,000", ZDNet. Retrieved 10 November 2011. As of 19 February 2012: http://www.zdnet.co.uk/news/security-management/2011/08/30/facebook-bug-hunting-scheme-pays-out-40000-40093785/

Ministry of Security and Justice (2011). The National Cyber Security Strategy (NCSS): Strength through Co-operation. As of 13 February 2012: http://www.govcert.nl/binaries/live/govcert/hst%3Acontent/actueel/nieuws/nationale-cyber-security-strategie-gepresenteerd/nationale-cyber-security-strategie-gepresenteerd/govcert%3AdocumentResource%5B3%5D/govcert%3Aresource

Mitchell, K. J., L. M. Jones, D. Finkelhor, J. Wolak (2011). "Internet-facilitated commercial sexual exploitation of children: findings from a nationally representative sample of law enforcement agencies in the United States", *Sex Abuse,* 23(1), pp. 43–71

Mott MacDonald (2002). "Review of Large public Procurement in the UK". As of 17 February 2012: http://www.hm-treasury.gov.uk/d/7(3).pdf

National Institute for Standards and Technology (2010). NIST Cloud Computing Programme. As of 15 February 2012: http://www.nist.gov/itl/cloud/

New Legal Review (2011). "ICANN teams up with Interpol to combat cybercrime" Retrieved 10 November 2011. As of 17 February 2012: http://www.cpaglobal.com/newlegalreview/4880/icann_teams_up_with_interpol_t

OECD (2008). "Malicious software (malware): a security threat to the Internet economy". As of 17 February 2012: http://www.oecd.org/dataoecd/53/34/40724457.pdf

OECD (2001). "The hidden threat to e-government: avoiding large government IT failures", OECD Public Management Policy Brief No. 8, March 2001. As of 15 February 2012: http://www.oecd.org/dataoecd/19/12/1901677.pdf

Paget, F. (2011). "Responses to cybercrime in Japan and France", McAfee Labs blog. As of 17 February 2012: http://blogs.mcafee.com/mcafee-labs/responses-to-cybercrime-in-japan-and-france.

Parlament České republiky (2011). Resolution No. 564 approving the Czech Cyber Security Strategy for the Period 2011–2015 (20 July 2011)

PR Newswire (2011). "Pandalabs uncovers alarming statistics on cyber-crime black market". As of 19 February 2012: http://www.prnewswire.com/news-releases/pandalabs-uncovers-alarming-statistics-on-cyber-crime-black-market-114270849.html

Qualye E, and T. Jones (2011). "Sexualised Images of Children on the Internet", *Sexual Abuse: A Journal of Research and Treatment,* 23(1), pp. 7–21

RIPE NCC (2012). "IPv6 Act Now". As of 15 February 2012: http://www.ipv6actnow.org/info/faqs-2/

Robinson, N., L. Valeri, J. Cave and T. Starkey (2011). "The Cloud: understanding the security, privacy and trust challenges", Santa Monica, CA: RAND Corporation. As of 19 February 2012: http://www.rand.org/content/dam/rand/pubs/technical_reports/2011/RAND_TR933.sum.pdf

Schmid, A. P. and A.J. Jongman (2005). *Political terrorism: a new guide to actors, authors, concepts, data bases, theories, and literature*, New Brunswick: Transaction Publishers

Sentencing Guidelines Council Secretariat (2007). "Definitive Guidelines on the Sexual Offences Act 2003", London. As of 19 February 2012: http://sentencingcouncil.judiciary.gov.uk/docs/web_SexualOffencesAct_2003.pdf

Singel, R. (2011). "Congress authorizes Pentagon to wage Internet war", Threat Level blog, *Wired*, 14 December 2011. As of 19 February 2012: http://www.wired.com/threatlevel/2011/12/internet-war-2/

Sommer, P. and I. Brown (2011). "Reducing systemic cybersecurity risk". As of 19 February 2012: http://www.oecd.org/dataoecd/57/44/46889922.pdf

Swire, P. (2009). "No cop on the beat: underenforcement in e-commerce and cybercrime", *Journal of Telecommunications and High Technology Law Review,* 107, pp. 107–126

Symantec (2010). Symantec Global Internet Security Threat Report: Trends for 2009, Volume XV. As of 19 February 2012: http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf

The Economist (2007). "Newly nasty: defences against cyberwarfare are still rudimentary. That's scary". As of 19 February 2012: http://www.economist.com/node/9228757

United Nations Office on Drugs Crime (2010). "Draft topics for consideration in a comprehensive study on the impact of and response to cybercrime", Expert group on Cybercrime, Vienna (UNODC/CCPCJ/EG.4/2011/2). As of 19 February 2012: http://www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/UNODC_CCPCJ_EG4_2011_2/UNODC_CCPCJ_EG4_2011_2_E.pdf

US Army (2005). "Cyber operations and cyber terrorism training and doctrine command 2005", TRADOC G2 DCSINT Handbook No 1 02. As of 15 February 2012: http://www.au.af.mil/au/awc/awcgate/army/guidterr/sup2.pdf

Valeri, L. , G. Somers, N. Robinson, H. Graux and J.Dumortier. Handbook of Legal Procedures of Computer and Network Misuse in EU Countries. Santa Monica, CA: RAND Corporation, 2006. http://www.rand.org/pubs/technical_reports/TR337.

van Eeten, M.J.G., J. M. Bauer with contributions by M. de Bruijne, J. P. Groenewegen, and W. Lemstra, Economics of Malware: Security Decisions, Incentives, and Externalities, *OECD STI Working Paper 2008/1 JT03246705*, Paris, OECD, 2008, available online at http://www.oecd.org/dataoecd/53/17/40722462.pdf.

Wall, D. S. (2001). *Crime and the Internet*. London: Routledge.

Wall, D. S. (2011) Policing Cybercrimes: Situating the Public Police in Networks of Security Within Cyberspace (Revised Feb 2011) *Police Practice and Research: An International Journal* Vol. 8 No. 2 pp 183-205 May 2007

Willis, H., Lester G. and Treverton, G. (2009). Information Sharing for Infrastructure Risk Management: Barriers and Solutions. *Intelligence and National Security*, 24(3):339-365(27)

WODC (2010). *European Sourcebook of Crime and Criminal Justice Statistics – 2010, fourth edition*. Den Haag: Boom Juridische uitgevers. *Onderzoek en beleid* series, no. 285, Ministry of Justice, Research and Documentation Centre, 2010. As of 16 February 2012: http://europeansourcebook.org/ob285_full.pdf

Yar, M. (2006) *Cybercrime and Society*. London: Sage.

APPENDICES

Appendix A: Participating organisations

Country	Units interviewed	Number of interviewees
Belgium	Federal Computer Crime Unit, Judicial Police	1
Cyprus	Office for Combating Cybercrime, Cyprus Police	2
Finland	National Bureau of Investigation, Ministry of Interior	3
France	Gendarmarie Cybercrime Division (GCD) France National Cyber Crime Investigation Unit (OCLCTIC)	5 5
Germany	High-Tech Crime Unit – BKA SO-43	2
Ireland	High-Tech Crime Unit – Garda ECTEG – University College Dublin	2
Italy	Postal and Communications Police	2
Luxemburg	Technical and Scientific Police and New Technologies Units, Judicial Police Service	2
Netherlands	National High-Tech Crime Unit, National Crime Squad, Netherlands Police Services Agency (KLPD)	2
Poland	Cybercrime Unit, Criminal Bureau of Investigation	3
Romania	Cybercrime Unit, Ministry of Administration and Interior	3
Slovenia	Computer Investigation Centre, Criminal Police Directorate	2
Spain	High-Tech Crime Unit, National Police	2
Sweden	Information Technology Crime Unit, National Bureau of Investigation	1
United Kingdom	Serious Organised Crime Agency (SOCA)	1

EU-level organisations	Number of interviewees
Europol	6
Eurojust	3
CEPOL	1
ENISA	3
CERT–EU Pre-Configuration Team	2

Industry	Number of interviewees
Google	1
Microsoft	3
Facebook	1
Ericsson	2
HSBC	1

Others	Number of interviewees
Council of Europe	1
Interpol General Secretariat	2
Internet Corporation for Assigned Names and Numbers (ICANN)	3
RIPE	1
APWG	2

In addition, to further triangulate our findings we also attended the following events:

- Second Meeting of the EU Cybercrime Task Force (EUCTF) held 21–22 June 2011, in The Hague, the Netherlands
- Joint ENISA–Europol workshop on CERT–LEA co-operation held 3–4 October 2011, in Prague, Czech Republic
- Council of Europe Co-operation against Cybercrime Conference, 21–23 November 2011, in Strasbourg, France
- Federal Foreign Office of Germany conference on Cybersecurity: Risks, Challenges and Opportunities held 13–14 December 2011, in Berlin, Germany

Attendance at these events was not part of the formal evidence-gathering framework of the research but rather provided cost-effective opportunities to discuss topics further, informally, and to validate findings via expert opinion.

Appendix B: Methodology

Methodology and approach

In order to answer the questions posed by the European Commission the research team devised an approach that aimed to gather and synthesise expert views of all relevant stakeholders at national and EU levels. This approach stems from the fact that cybercrime is a multi-stakeholder issue.

In particular it is important to understand how poor cybersecurity makes cybercrime possible (for example see Anderson, 2008). Providing for levels of cybersecurity, however, requires the active participation of different stakeholders who each have a responsibility to act. This is in contrast to fighting cybercrime which has a more focused remit (gathering intelligence, prosecution of cybercriminals) and fewer stakeholders (law enforcement, judiciary and public prosecutors).

The methodology is illustrated in Figure B.1:. This shows that the research approach was broken down into two stages.

Stage 1

The objective of the first stage was to:

- Examine and report on the current state of the art regarding cybercrime and national and international police and law enforcement responses.
- Understand existing law enforcement and non-law enforcement methods to report, process and handle cybercrimes.

Undertaking a literature review

The literature review involved a series of tasks:

- Identification of academic literature based the following keywords:
    - cybercrime (OR cyber-crime OR cyber crime) AND cyber security
    - cybercrime (OR cyber-crime OR cyber crime) AND policing
    - cybercrime (OR cyber-crime OR cyber crime) AND measurement
    - cybercrime (OR cyber-crime OR cyber crime) AND reporting
    - cybercrime (OR cyber-crime OR cyber crime) AND statistics
- Summary of the articles and reports retrieved across the following research questions:

- What is the current state of the art regarding cybercrime across the Union and other countries?
- Is the prevalence of cybercrime increasing or decreasing? Do we know? If we cannot reliably tell, why?
- What are the issues associated with measuring this phenomenon?
- What are governments doing about it?
- What law enforcement-based reporting systems exist in each MS?
- What are the resource implications with such reporting systems?
- How do such national capabilities interact with other relevant institutional actors?
- How successful have they been in measuring the extent of this phenomenon?
- To what extent are awareness and prevention activities effective?
- How do these reporting systems contribute to other national efforts to improve cybersecurity?
- What role does the private sector play?
- Is reporting of cybercrime legally mandated in MS?
- What are the current role and capabilities of Europol, ENISA, Eurojust and CEPOL?

The findings from the literature review so far are set out in Chapter 1.

Conducting face-to-face interviews with the heads of Member State law enforcement unity dealing with cybercrime

We conducted in-depth fieldwork-based site visits to 15 countries from across the Union. These countries were selected on the basis of those which we envisaged would allow us to discern the most breadth and range of law enforcement responses to cybercrime. The selection matrix can be found in Appendix B. The selection was intended to include 15 countries that represented a spread across the selection variables. The countries in which interviews were conducted are listed in Box B.1. Findings from the interviews are set out in Chapter 3.

Box B.1: Member States selected for case study interview

1. Belgium
2. Cyprus
3. Finland
4. France
5. Germany
6. Ireland
7. Italy
8. Luxembourg
9. Poland
10. Romania
11. Slovenia
12. Spain
13. Sweden
14. Netherlands
15. UK

Conducting interviews with key informants from Europol, ENISA, CEPOL, and Eurojust

These have been completed. Findings from the interviews are presented in Chapter 4.

Stage 2

The objective of stage 2 of the research is to use the results of the evidence-gathering to determine the best way to implement an ECC and its most appropriate configuration.

Methodology for options development

To develop the options we considered a matrix of the different ways each objective identified from the fieldwork (and also via previous inputs) could be achieved. These routes to delivering these objectives were based on a spectrum of types of tasks, namely operational > collaborative > advisory. Stakeholders of different types and different levels (the four core EU stakeholders, Member States and the private sector of different types) all have different strengths and weaknesses across each type of tasks.

This has been completed and the options arising from the data collected so far and the gap analysis are set out in Chapter 6.

Stakeholder workshops

Europol, Eurojust, the European Network and Information Security Agency (ENISA) and CEPOL have been identified by the European Commission as key stakeholders in discussions about the creation of an ECC. The research team undertook visits to each organisation to conduct a workshop or roundtable discussion with representatives from each of these organisations. In this discussion each of the options was reviewed and discussed in terms of its feasibility and strengths and weaknesses.

The workshops were conducted during October 2011.

Final workshop

A final broader workshop took place at the end of the study in November 2011. This workshop validated the findings of the study so far, and explored more specifically the different options that resulted from the discussions, as well as considerations as to their feasibility. Following presentation and discussion of the results, a moderated "foresight" exercise took place to compare the empirical evidence against a longer-term perspective of a future that is by definition uncertain, to assess which options are the most "robust" options going towards that future.

Figure B.1: shows how each of the data collection methods were used to answer the research questions posed by the Commission.

Figure B.1: Overview of research approach

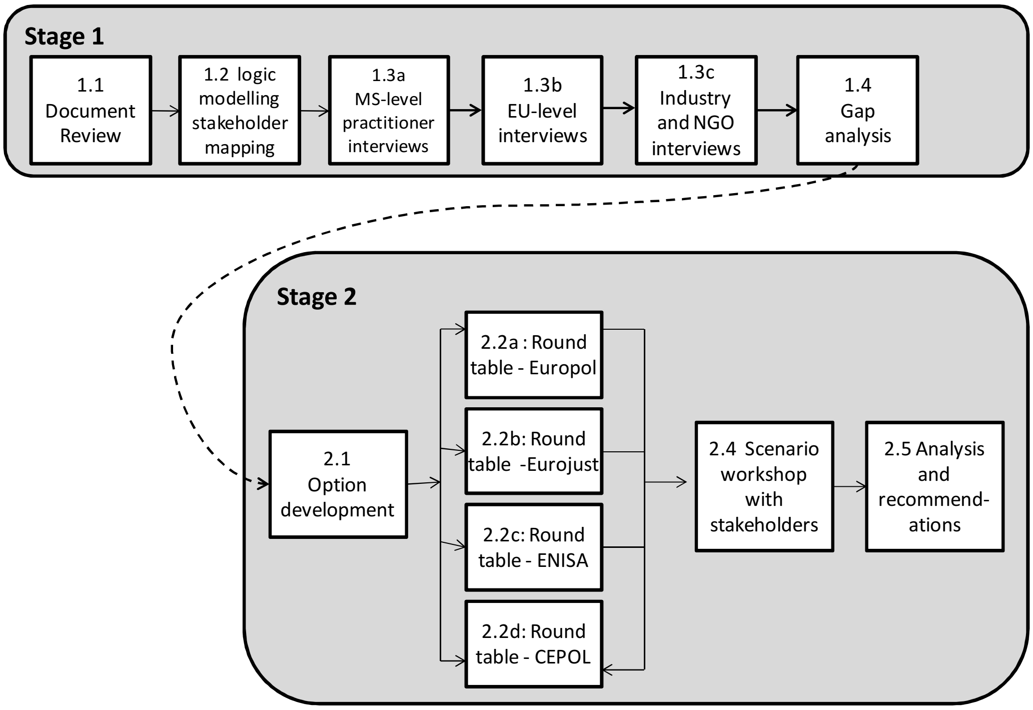

Stage 1
1.1 Document Review
1.2 logic modelling stakeholder mapping
1.3a MS-level practitioner interviews
1.3b EU-level interviews
1.3c Industry and NGO interviews
1.4 Gap analysis
Stage 2
2.1 Option development
2.2a : Round table - Europol
2.2b: Round table -Eurojust
2.2c: Round table - ENISA
2.2d: Round table - CEPOL
2.4 Scenario workshop with stakeholders
2.5 Analysis and recommend-ations

Table B.1 Summary of methods used to answer each of the research questions posed by the Commission

Research question	Literature review	Fieldwork
What is the current state of the art regarding cybercrime across the Union?	Y	Y
Is the prevalence of cybercrime increasing or decreasing? Do we know? If we cannot reliably tell, why?	Y	
What are the issues associated with measuring this phenomenon?	Y	
What are governments doing about it?	Y	Y
What law enforcement-based reporting systems exist in each Member State?		Y
What are the resource implications with such reporting systems?	Y	Y
How do such national capabilities interact with other relevant institutional actors?		Y
How successful have they been in measuring the extent of this phenomenon?		Y
To what extent are awareness and prevention activities effective?	Y	Y
How do these reporting systems contribute to other national efforts to improve cybersecurity?		
What role does the private sector play?	Y	Y
Is reporting of cybercrime legally mandated in MS?		Y
What are the current role and capabilities of Europol, ENISA, Eurojust and CEPOL?		Y

Interview discussion guide

For each meeting with either a Member State cybercrime unit, an EU level institution or industry representative we used the following discussion guide below. This was tweaked in certain circumstances (e.g. for industry we omitted the questions concerning contribution to AWFs).

Section 1: Context

1. Please describe the background to your unit and where your unit fits within the overall criminal justice response in your country
2. Please indicate the mandate of your organisation and whether it has any specific legal or regulatory basis?
3. Please describe the organisational structure of your unit, including operations, management, support etc
4. Please could you describe any elements of the cyber crime environment or situation in [country] which affect the prevalence or cyber crime, or which impact upon your organisation's response to cyber crime?

Section 2: Inputs

1. Please indicate your annual overall level of resourcing - how many full-time equivalent staff does your unit have and what is your total yearly budget?
2. Please could you elaborate on the ratio of FTE between managerial/senior professional/analyst and administrative/secretarial staff
3. Please indicate the staff profile (e.g. analysts, technical support, managerial, public outreach) in your organisation. Are these drawn from exclusively law enforcement community?
4. Do you collaborate with other organisations which provide inputs to your unit? For example, private sector organisations which collect relevant data and the centre or other departments (which essentially comes down to a pooling of resources)?
5. Are there any other important inputs to your organisation which we've not asked about?

Section 3: Processes

1. It would be very helpful to get an overview of the main activities undertaken by [unit]. We have listed some possible activities in this table. Please could you indicate which, if any, apply to your organisation – of course adding any we have not included – and say a little about each of these?

Detection, investigation and prosecution of serious forms of cybercrime (as defined by the Budapest Convention) including court appearances, interaction with other MS/ Third countries
Operating and running a hotline
Production of intelligence

Forensics
Training
R&D (technical and also investigative techniques e.g. social network theory)
Outreach (e.g. running education and awareness raising campaigns; visiting schools or other community venues etc)
Links with Europol (e.g. acting as Europol National Unit)
Submitting information to Europol via SIENA (if possible, please indicate of quantity of traffic transmitted)
Any other activities

2. Are there any activities which your unit does not undertake, but you think that it should?

Section 4: Outputs

1. What metrics, if any, do you use to monitor outputs and outcomes of [organisation]?
2. What is your opinion as to the quality of the data available for these metrics?
3. Please describe any reporting your unit is expected to produce? How often must reports be prepared? Who are they sent to? How are they scrutinised?
4. Are they any legally mandated requirements for your unit to submit data, for example, to a centralised national criminal justice statistical agency, or externally to organisations such as Europol
5. Could you please say a little about the key outputs from your main activities and processes?

Activity	Possible examples of outputs?
Detection, investigation and prosecution of serious forms of cybercrime (as defined by the Budapest Convention) including court appearances, interaction with other MS/ Third countries	Numbers of prosecutions; Number of investigations started; number of investigations leading to prosecution etc. Please indicate the number of investigations that result in successful prosecutions Please provide information on realised sanctions against those successfully prosecuted Please indicate the variation year on year, of reported incidents or investigations or prosecutions?

Operating and running a hotline	number and motive of callers); number of cyber-incidents reports yearly; number of different cyber incidents reported yearly;
Production of intelligence	
Forensics	
Training	Number of training courses delivered; awareness and outreach activities performed;
R&D (technical and also investigative techniques e.g. social network theory)	
Outreach (e.g. running education and awareness raising campaigns; visiting schools or other community venues etc)	
Links with Europol (e.g. acting as Europol National Unit)	
Submitting information to Europol via SIENA	Quantity of traffic transmitted?
Any other activities	Other outputs?

1. **Section 5: Outcomes and impact** What is your assessment of the impact of your organisation on cyber crime? What is the basis of this assessment?
2. Based upon available data, has the prevalence of recorded cybercrime in your country/area of responsibility increased or decreased since your unit has been operational?
3. Do you think the work and activities of your organisation have impacted upon overall levels of cyber crime? If not, what has driven levels of reported cyber crime?
4. Please describe, if any, your approach to evaluation of your activities? Is your centre subject to external evaluation?

Would you like to add anything else about the impact and outcomes of your unil in relation to cyber crime in [country]

Appendix C: Country reports

In this Appendix we present summaries of the discussions in respect of findings from the Member States.

Belgium – Federal Computer Crime Unit (FCCU), Judicial Police

Context

The presence of many EU institutions in Belgium may make it an attractive target for cybercriminals. Currently, hactivist organisations such as Lulz Security (LulzSec) are thought to pose a significant threat. The yearly economic impact of cybercrime in the country is estimated at €1 billion.

The Federal Computer Crime Unit (FCCU) is part of the Federal Police (under the Ministry of the Interior). It interacts with Regional Computer Crime Units (RCCUs).

The Unit's mandate comes from the law on Integrated Police (from the Police Reform initiative of 2001). The objectives and goals of the FCCU stem from the National Security Plan 2007–2011, supporting the development of the National Police Crime Image Picture. FCCU's focus relies on a strict definition of cybercrime that considers only those crimes where the computer is a target and not the means, such as hacking, Internet fraud, and e-banking fraud. The unit's concern is on where cyberspace has been abused or modified, and thus activities such as Internet based Mass Market Fraud (IMMF) do not constitute cybercrime in its view.

The FCCU works on a reactive basis in response to requests from RCCUs. Unlike the internal investigations unit, it does not have any autonomous investigative capability. FCCU also supports other analyses of how criminals use ICT to anonymise their activities and run their businesses.

The unit is currently split into three divisions: Policy, Intelligence, and Operations. However, under internal reforms they are trying to merge these into one.

Input

In 2011, FCCU had 33 full time employees. There were 249 staff members employed in the RCCUs. Though resourcing is currently decreasing, the staff profile is also changing, reflecting the growing requirement for BA and MSc in forensics. Staff are typically recruited through the police system or through specialised recruitment. The FCCU also provides specific training. The 2011 budget was €750,000.

Processes

FCCU activities include co-ordination, policy input, support, and intelligence. FCCU intelligence-gathering and forensic investigations occur at one of three levels. The first addresses active files on Windows or Linux file systems, the second involves the recovery of e-mail logs and the like, and the third involves the recovery and analysis of deleted and wiped data at the hardware level. The unit also completes network forensics of traffic data streams in real time, a task that requires considerably more expertise. Additionally, the unit also handles ID requests from Microsoft, Google, Facebook and other industry stakeholders.

FCCU collaborates with the B-CCENTRE, Europol, industry stakeholders and ENISA. The unit also maintains links with CERTs.

Outcomes and impact

Challenges persist in measuring both the impact of cybercrime and of FCCU activity. Obtaining data is made more difficult by the fact that there is no means to detect or report incidents of cybercrime. Other challenges arise from the fact that the centralised police database is not adapted to updating records relating to cybercrime.

Cyprus – Office for Combating Cyber Crime (OCCC)

Context

Understandings of cybercrime in Cyprus are widely construed, with law enforcement handling issues ranging from hacking to online suicide threats. Of these varied issues, the most serious cyber threat in the country is the publication of child pornography hosted in third countries.

The Cyprus police force is distributed throughout the country's six geographical regions. The Office for Combating Cyber Crime (OCCC) is a centralised unit dedicated to countering child pornography and hacking. It was established in 2007, with the forensics lab becoming a separate unit within the same structure in 2009. It operates within the legal framework of the Budapest Convention to assist and provide investigative support for the financial crime unit. The unit sits under the administration of the Ministry of Justice, and the two organisations work closely with one another. The Office of the General Attorney has a prosecutor specifically dedicated to cybercrime. The OCCC investigates offences committed against computer systems and data as well as offences committed through or by means of computer systems.

Input

The OCCC is staffed by six investigators and seven technicians, all of whom graduated from the Cyprus police academy.

Processes

The OCCC is responsible for collecting electronic evidence to support its own and other investigations. The office can seek support from the Computer Forensic Examination Lab in serious cases. The unit performs all forensics except for telephone and CCTV work. It also sends members to international training programmes and runs training courses on cybersecurity for the private sector. The centre's R&D role is limited, though it does develop some databases. The unit has no intelligence capability, but it does engage in some preventative efforts.

The unit collaborates closely with several organisations internationally. It submits data to AWF Cyborg. Liaison Officers have also worked with the FBI, as well as officials in Greece, Germany and the United Kingdom. The latter hosts three SOCA officers in Cyprus.

Output

The unit records all the cases it processes in a given year and their outcome and contributes to annual and monthly reports. In 2010, it provided information on child pornography to other countries in 236 instances and conducted nine child pornography cases of its own. The unit also ran 55 investigations involving illegal access, interception and interference, and 39 cases involving computer-related forgery.

Outcomes and impact

Co-ordinating and obtaining contributions from third countries continues to be a challenge, with bureaucratic procedures creating long time delays or adding complexity.

Finland – Financial Crime/IT Crime, Criminal Investigation, National Bureau of Investigation

Context

Cybercriminality in Finland is understood to include criminality facilitated by the cyber world, a somewhat wider definition than that used in some other countries. The country's proximity to Russia and the Baltic states also creates specific conditions relating to cybercrime. Many Russians live in Finland and perpetrate crimes there against others. Many come across on the ferry from Estonia and execute "hit and run" trips involving ATM-skimming.

Finland's relatively small size also affects how it deals with cybercriminals and agencies. Interactions with industry and Computer Emergency Response Teams (CERT) tend to be via personal contacts. CERT.fi is very good at addressing vulnerabilities before they get to law enforcement agencies, thereby pre-emptively lessening the police workload. The fact that the language is spoken by a relatively small number of people also helps discourage crime.

Legally, law enforcement agents have an obligation to act except in those cases in which the victim chooses to press charges. Police must pay for requests to telecommunications companies and are allowed to conduct surveillance and undercover operations in limited circumstances. Generally, there exists a perception that the criminal justice system and the legislation protects the perpetrator rather than the victim.

The cybercrime unit sits within the National Bureau of Investigation (NBI), under the Ministry of the Interior. The NBI has three Directorates: Intelligence, Investigation and Lab, which provides forensics support. The cybercrime capability in the NBI is a kind of matrix system, built up from the three capability units within the NBI. The Intelligence Unit works on prevention and international co-operation, the latter with Europol and Interpol. The Investigation Division sits alongside economic crime, organised crime and homicide, and serious crime against the person, while the lab has an R&D function. Each of the 24 police districts in Finland has between one and three forensic specialists plus other police officers knowledgeable about cybercrime but not specifically allocated as such, nor is there a single "head" of the cybercrime unit in Finland.

Inputs

The Investigation Division has 10 full-time employees, the Intelligence Division 14, and the R&D lab three. The unit is allocated €100,000 a year for hardware and an additional €100,000 for training. Foreign-language translation is a significant cost. The unit is trying to double its resources as a result of public pressure. In addition to the collaboration with CERT.fi, the unit collaborates with the banking sector via personal contacts.

Processes

As regards the detection, investigation and prosecution of serious forms of cybercrime, the NBI uses three criteria to determine the follow-up of reported crimes. These include whether the NBI can launch an investigation, whether the crime is Internet-related and whether there is an international dimension. The lack of cybercrime evidence in Finland, strictly construed, has led to a greater effort spent on addressing computer-mediated crimes.

A crime hotline run by the police receives about 10,000 tips per year, not all of which are related to cybercrime. Of these, 2,000 go toward successfully solving a case. The unit is primarily operational in focus and does not provide training. Training is obtained from external sources at significant cost.

Links to Europol are largely devolved, with each unit in the Intelligence Division submitting its own data to Europol via separate links. Finland was the largest contributor to AWF Cyborg last year (perhaps because of the tendency to provide all relevant data of a cybercrime case) but at the time we spoke to them had yet to contribute anything for 2011. Collaboration also occurs with Interpol and the Nordic forum on IT issues. Joint Investigation Teams with third countries have also proven effective, as they have greatly increased the speed with which requests are processed. Liaisons with the three national prosecutors dedicated to cybercrime issues are improving.

Outputs

In addition to the 2,000 cases that originate in tips from the hotline, the NBI conducts roughly 100 investigations concerning drugs, firearms or fraud, 50–70 on online child exploitation, and 20 at the request of banks and the private sector each year. In 2010 there were 16 new cases, 11 of which were solved. In 2011 to date (in mid 2011), there are 14 cases open. Roughly 20 new cases per year half are related to money-laundering. As regards forensics analysis, the NBI seizes and analyses roughly 60TB of data across all types of crime commodities. The unit also conducts some R&D work, notably in the form of the Collabro project under the ISEC programme.

Outcomes and impacts

There is no reporting requirement for cybercrime in Finland. Acquiring statistics proves a challenge for two reasons. Firstly, because the CERT is funded by industry, they do not share their statistics. Secondly, statistics are often grouped by topic (e.g. fraud). Cyber is not a qualifying feature in these reports.

As cybercrime is beginning to receive more attention in Finland, it is hoped that the compilation of statistics and other relevant information will improve. Police continue to focus on preventing child exploitation and on using the Internet as an investigative resource.

Though Finnish officials note that, when it comes to European collaborative forums, the wheel is constantly being reinvented, they do hope to push for greater collaboration in the future, such as in the form of a common approach to mass-market fraud. More analysis support from Europol itself would also prove useful.

France – Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication (OCLCITC) and Gendarmerie Division de lutte contre la cybercriminalité (GCD)

Context

Law enforcement in France is divided between the police and the gendarmerie. The latter were formerly part of the Ministry of Defence but are now attached to the Ministry of the Interior. The Gendarmerie's jurisdiction covers half the population outside of cities.

The OCLCTIC was created in 2000 to provide a centralised agency to address cybercriminality issues, investigate or provide assistance for cases involving a cyber/ICT dimension, and advise the Minister of the Interior on those issues. Its activities centre on three aspects: investigation, an online reporting platform, and technical assistance and training.

The Gendarmerie's Division evolved from the IT forensics lab put in place in 1992. The Division works in close co-operation with the Gendarmerie's Forensic Department, which sits under the judiciary centre of the Gendarmerie.

Both agencies focus on cybercrime, not cybersecurity. This is the remit of ANSSI (Agence nationale de sécurité des systèmes d'information), CERTs and the DCRI (Direction centrale du renseignement intérieur). It is also important to note that there are between three and five units dealing with cybercrime in France, each with a different specialty, leading to difficulties in co-ordination or establishing the total number of individuals working on cybercrime.

Input

The OCLCTIC is staffed by 50 people: 11 for operations, 14 (Pharos), three (*Info-escroqueries*) for the reporting platforms, three for training, and 19 dispatched to other units. There is no defined budget at the unit level. Rather, resources are requested and assigned on the basis of necessity.

The Gendarmerie staffs 25 people: nine general investigators, nine investigators specialised on child abuse, five individuals providing telephone and other support, one head of Division and one deputy. The unit has no defined budget, but plans expectations for equipment on a yearly basis.

Overall, France has 298 Police and 250 Gendarmerie cybercrime investigators on both the national and local level.

Processes

The OCLCTIC works closely with prosecutors to decide which cases to open or follow. The centre has three main streams of activities:

1. Operational activities and investigations
2. Pharos (created in 2008), a reporting platform for the public and users of the Internet to signal misuse and legal infringements. Pharos has both a centralising and a triage function.

3. Providing technical assistance and training. This includes the implementation of a national training programme for cybercrime investigators (material from ECTEG) and assistance for forensics, Internet watch (i.e. social networks) support to criminal investigations with an IT element, R&D.

The OCLCTIC is also the point of contact for Interpol. It maintains links with industry and with ISPs. It also contributes to SIENA and maintains bilateral relationships. Regarding Cyborg, the level of contribution depends on the cases being followed.

The Gendarmerie has three main lines of activity:

1. Online investigations. These involve surveillance campaigns lasting one or two weeks focusing on a particular topic such as drugs, illegal gambling, counterfeit goods, and take place four or five times a year.
2. Investigation into online child abuse: This is a joint effort conducted with the police and also involves providing evidence and information to national and Interpol databases.
3. Provide support to other units of the Gendarmerie on ISP-related issues.

The division also takes part in prevention campaigns and provides information to Twins. As regards co-operation, the division co-operates with OCLCTIC, other specialised units of the police, ARGEL (online gambling) the CNIL and Hadopi, ANSSI and industry. The Forensics Department has three primary activities: data extraction, data analysis, and support to crimes with IT components.

Output

OCLCTIC runs a four-week training programme three times per year. It trains 54 people a year in this fashion, but this number is expected to increase.

The Gendarmerie, in conjunction with the Université de Troyes, provides a four-year training to obtain a *license professionnelle* (professional bachelor) as well as a Masters in IT security. To date 250 people have been trained.

Outcomes and impact

The OCLCTIC finds it difficult to estimate its impact as there is limited feedback from the local services. The unit is developing statistical and feedback tools.

The Gendarmerie does not have any serious statistics on French cybercrime. In comparison with other crimes, the number of cases in cybercrime refers to the level of effort and resources invested, rather than the level of crime itself.

Germany – Federal Criminal Police Office (BKA) SO43 – Cybercrime

Context

Policing in Germany operates at state (*länder*) level. The Bundeskriminalamt (BKA) operates at federal level together with the border guards and the unit for the protection of Parliament. The BKA has no power to give orders to the state police, but rather works with them in a state of permanent collaboration. The BKA itself is specifically tasked to intervene in those cases involving drugs, weapons, false money, terrorist attacks and cybercrime.

The BKA can also conduct its own prosecutions, but it must first be asked by the public prosecutor to take a case forward. Prosecutors thus decide which police cases should be followed. Finding prosecutors specifically dedicated to cybercrime has proven challenging in the past, however currently a working group near Frankfurt consists of three special prosecutors dedicated to the issue. There further exists a strict organisational separation between police and intelligence agencies in Germany.

Nine operational divisions make up the BKA. SO43, the BKA's high-tech crime unit, is itself made up of four sections: policy support, operational analysis and statistics, random Internet searches, and investigations. It focuses on attacks against data or data systems, and particularly on botnets.

Inputs

SO43 employs 43 people. Of these, six work in Policy, 12 in Operational Analysis and Statistics, 10 in random Internet Searches, eight in searches, eight in investigations, and the remainder in headquarters or administrative roles. The unit requested an additional 16 staff members in 2008, but these have yet to be obtained.

The unit operates on a centralised budget for travel and subsistence. Its proposed IT budget was €280,000 for hardware and software licences and specialised computer equipment.

Processes

In addition to conducting investigations, SO43s also delivers training, an average of two people on the unit continuously delivering training or presentations to IT companies and national stakeholders.

The unit is also increasingly involved in collaborative or co-operative efforts with private-sector stakeholders. Accordingly, SO43 has forged links with private-sector companies involved in Internet security or with business models linked to the Internet, such as banks, credit card companies, anti-virus firms, ISPs, and telecommunications firms. This co-operation takes many forms and has involved aspects of reporting, information-sharing and outreach. At a strategic level, dialogues between the German association of ISPs, SO43 and wider BKA have taken place regarding access to IP addresses and the feasibility of operating 24/7 contact points. Law enforcement and the private sector are also trying to establish an institutionalised PPP where the BKA and private sector representatives could be housed in the same building but not necessarily in the same organisation. Currently, information is shared between the public and private sector three or four times a year, but the goal is to establish daily – or at least more regular – personal contact and exchange. For this to happen, the police must demonstrate to the private sector that they can effectively manage cases involving cybercrime and add value while doing so. Moreover, the processes of reporting and the operations of BKA need to be clarified for private-sector audiences.

SO43 participates in the 124/7 network at Interpol, but the individuals involved are not on long-term contracts, resulting in a loss of learning over time. The BKA currently has standing as an observer on Europol's AWF Cyborg.

Output

The BKA produces cybercrime statistics for its own reporting system. There are also National Crime Statistics, however in these it is sometimes difficult to distinguish cybercrime from other cases of fraud. Every three or four months, the BKA publishes a cybercrime bulletin to raise awareness within the *länder*.

Outcomes and impact

Investigations and successful arrests provide some indication on the levels of cybercrime within Germany. For example, there were a number of cases in which there were roughly 1,000 successful transfers of phishing of which the BKA was previously aware of 300–400. From these cases, the BKA has determined that it is aware of about 30 percent of the instances of cybercrime in the country. Investigations are often found to have a short-term effect (three or four weeks) in lessening crime, but their impact is difficult to assess in the long term.

Officials within SO43 consider the regularisation and harmonisation of practices between MS as an area in which the ECC might potentially prove useful. An EU-level operational capability could also assist in collating and co-ordinating information requests.

Ireland – High-Tech Crime Unit (HTCU), Garda and the European Cybercrime Training and Education Group (ECTEG) at University College Dublin

Context

The High-Tech Crime Unit (HTCU) sits within the Fraud Investigation Division of the Garda.

Inputs

HCTU employs 13 full-time staff of detective grade or higher, as well as an additional three detectives on secondment from the paedophilia investigation unit. All staff are trained at University College Dublin (UCD) and possess an academic qualification. The unit also makes use of computer scientists at UCD. There is no ring-fenced budget for the HTCU. Rather, funds are requested from the Fraud Investigation Division on an ad-hoc basis.

Processes

HCTU provides forensics and investigative support to local policing units. The unit undertakes forensic examination of all digital media and also has responsibility for investigating high-tech crime in Ireland. In a given year, the unit receives between 650 and 700 requests for assistance, with these varying in scope from the examination of a single computer to providing information about a child exploitation network with many members. On average, the unit examines 14 computers per case. HCTU has the capacity to examine an average of 400 cases a year.

The HCTU works with the private sector by participating in an information-sharing and analysis forum with retail banks based in Ireland and ISPs. They are in the process of developing a similar forum for telecommunications stakeholders.

The unit also acts as the point of contact for Interpol and Europol, from which it receives alerts and requests for assistance. These are often directed to computer scientists at UCD for analysis. The unit is also the SIENA reporting point.

A hotline exists for the public reporting of cybercrime in Ireland, but this is not operated by the police. HCTU does receive information reported to this hotline. The unit is also involved in outreach efforts, many of which involve other parts of the police.

A unique relationship exists between HCTU and UCD, particularly in regard to the European Cybercrime Training and Education Group (ECTEG). The two organisations have worked closely together since 1997, and are partners in Commission-funded projects to develop training for law enforcement officers in cybercrime investigation and digital forensics. UCD staff provide operational support to the HTCU and HTCU leadership currently sits on the board of ECTEG. UCD also works with other organisations in this field, notably the United Nations Office for Drugs and Crime (UNODC).

Outputs

The HCTU reports annually to the Head of the Fraud Investigation Division.

Outcomes and impacts

The view from within the organisation is that the collaboration with UCD has been successful, however its future is in jeopardy due to a lack of funding.

Officials within HCTU also find the high workload and current backlog of cases worrying. They also note that Ireland has yet to ratify the Cybercrime Convention. When it does so, law enforcement expect their workload to increase as there will be more offences to investigate, though these investigations will be facilitated by the advantage of having more appropriate offence definitions.

Training is another area which draws concern. ECTEG is running out of funding and its training materials are becoming out-of-date. Europol does not currently provide any training functions, however this may be a potential future role for the European Cybercrime Centre.

Italy – Postal and Communications Police (PCP); Italian National Police

Context

The Postal and Communications Police (PCP) is part of the Italian National Police, which sits within the Public Security Department of the Home Office. The PCP began in 1981 as a police unit dedicated to postal and communications protection. In 1998, PCP was mandated to develop the security and regularity of telecommunications services.

The PCP both conducts investigations and constantly monitors the Internet. Its main areas of investigation are: online child pornography, critical information infrastructure protection, cyberterrorism, home banking and electronic money, copyright, e-commerce, hacking, mail-related offences and counterfeit postage stamps, radio frequencies and electromagnetic pollution, online gaming and betting, providing operational co-operation with foreign law enforcement agencies, and support and training in digital forensics.

The central office ("Servizio") co-ordinates the activities of the PCP's 20 regional offices and 80 provincial sections. It also conducts investigations, evaluates strategies, and works with international partners.

PCP hosts three national centres: the National Centre Combating Online Child Pornography (CNCPO), the National Centre for Cybercrime and Critical Information Infrastructure Protection (CNAIPIC), and the Online Police Station.

Inputs

PCP's central office in Rome employs 144 full-time staff, while the regional offices employ an additional 1,822 individuals. Personnel are recruited from the National Police. The unit's budget comes out of the budget allocated to the Ministry of the Interior. It has no ring-fenced budget of its own.

Processes

PCP's three units conduct a wide range of activities in its efforts to counter cybercrime. CNCPO co-ordinates investigations and conducts image analysis and reports acquisition, monitors paedophile websites, and co-operates with international stakeholders and financial institutions. It is the only unit within the National Police that can undertake covert investigation in relation to child pornography and also has the power to blacklist illicit websites outside of Italy. CNCPO frequently co-ordinates with the Crimes against Children Observatory within the Prime Minister's Office, the Bank of Italy, ISPs, other law enforcement agencies, NGOs and other users.

CNAIPIC is responsible for preventing and combating computer-related crimes, including terrorist offences, against information systems and networks of national critical infrastructures. It has the power to conduct pre-emptive telecommunications interceptions and to perform undercover investigations. It runs a 24/7 Operational Room and intelligence analysis centre.

The Online Police Station is one of the first such instruments in Europe. It acts as a point of reference for information, advice, and expert interaction as well as a site of report submission. Its areas of focus include e-commerce purchase and sales, computer intrusion, phishing, unrecognised telephone traffic, and unauthorised online credit card use.

PCP works closely with international partners such as VGT, Europol, Interpol, Eurojust and Cospol. It is part of the G8's subgroup on High-Tech Crime and a member of the European Working Party on Information Technology Crime (EWPITC). It is the national contact point for international organisations and the point of reference for other Italian law enforcement agencies who want to freeze evidence in other countries.

Outputs

PCP collects daily data on its activities from the regional offices. From July 2010 to June 2011, the organisation made 47 arrests relating to child pornography, three arrests relating to computer crime, and 125 arrests relating to electronic money and e-commerce crimes, among others. PCP also conducts thousands of instances of online monitoring over the course of a year. There were 11,530 instances of such monitoring having to do with crime prevention of cyberterrorism alone from July 2010–June 2011.

During that same time period, the Online Police Station handled 14,668 requests for information and 14,018 crime reports. CNAIPIC conducted 5,253 instances of web monitoring and 63 investigations. CNCPO arrested 37 individuals in the first half of 2011 and blacklisted 141 websites.

Outcomes and impact

The PCP is fairly well known to the Italian public, leading to an increased likelihood that individuals will report instances of cybercrime. Members of the organisation felt that the PCP's work in combating child pornography has been particularly effective.

Luxemburg – Technical and Scientific Police Department and New Technologies Department, Judicial Police Service

Context

Cybercrime in Luxemburg mainly involves internationals making use of the country's botnet. The precise origin of these perpetrators remains unclear.

It is the prosecutors within the country that are responsible for centralising complaints and requests for investigations and then deciding which cases to investigate. Police then act reactively to these requests. Prosecutors receive written reports of cases directly from victims or via lawyers or the police. Their criteria for investigation are not explicit, but tend to include considerations on the severity of the crime, its international dimensions, the likelihood of being able to gather the necessary evidence, and the extent of the damage caused. A new prosecutor has just been appointed to focus explicitly on cybercriminal issues, with the intention that this appointment will help law enforcement separate cybercrime from the more general IT-facilitated crime.

The Technical and Scientific Police and New Technologies divisions were established in 2003, as developments in the area of cybercrime outpaced the capabilities of the economic crime unit. The New Technology section operates at a regional level, and its mission is to support forensics of IT-facilitated crime, investigate cybercrime, and to facilitate and conduct R&D in the technical aspects of telephone interception.

Input

The unit has 10 full-time employees, two of whom are mid-ranking law enforcement officers. It operates on a budget of €750,000, of which 60 percent goes toward intercepting data.

Processes

The unit conducts investigations of cybercrimes and analyses forensics related to cybercrime and IT-related crime. It also provides training in basic forensic capability to regional police forces. Detection, primarily via wiretapping, is another of its key activities.

As in the rest of the Luxemburg police, the unit does not conduct its own intelligence. Rather, communication with the intelligence community is conducted via the prosecutor's office, and normally revolves around the sharing of techniques and software.

The cybercrime unit maintains close bilateral collaboration with law enforcement agencies in Germany, Belgium and France. It also works with Europol and Interpol, though its contributions to AWF Cyborg are made only on an ad hoc basis.

Due to Luxemburg's small size, the New Technologies division is able to maintain good contacts with members of the private sector. Finally, the police have good relations with the country's three CERTs. One of these is for the government, another for the banks, and the third for the education sector.

Output

The division operates a database that allows it to monitor the time it spends on different cases and produces annual reports on its activities. Available data suggests that there is a 5–

10 percent increase in cybercrime specific cases each year, and that there is a 10–20 percent yearly increase in the support that the unit needs to provide in relation to cyber-related crime. In 2010, the unit handled 23 cases. At the time of data collection, there were an additional 11 cases as of October 2011.

Outcomes and impact

Officials within the New Technologies division anticipate that greater co-operation and speed in international collaboration will be necessary in the future.

Netherlands – National High-Tech Crime Unit (NHTCU) Team High-Tech Crime, Netherlands Police Services Agency (Korps Landelijke politiediensten)

Context

Owing it its high level of development and its extensive infrastructure, the Netherlands poses an attractive target for cybercriminals. For example, due to the popularity of the Amsterdam Internet Exchange, the country is seen as a good venue for server–hosting as there are fast connections with a number of other countries.

From 2005 to 2006, the National High-Tech Crime Centre operated out of Schipol airport. During that period, the centre focused on the tools that enable cybercriminality. The Centre at that time was not part of the national police.

The Dutch National High-Tech Crime Unit (NHTCU) was established in its current form in 2007. NHTCU is an operational unit of the national police and, as such, its mandate is set out in general Dutch legislation on law enforcement.

The organisation focuses on the phenomenon of cybercrime and its actors. Since 2009, NHTCU has developed a strategy of "surgical intervention," which involves a focus on high-impact, low-volume crime. The aim of this selective approach is to disrupt and deter major criminal operations – the "big fish" – rather than prosecuting every instance of criminal activity. NHTCU serves two purposes:

To investigate, prosecute and innovate with respect to national and international-level cybercrime issues.

To support the regional police forces in their own local and regional-level cybercrime issues.

Inputs

NHTCU is composed of four units, each employing about 30 full-time staff members. Staff are split evenly between technicians and police, though technicians undergo a rapid police training to enable them to work on investigations. To support its second, more regionally-focused, function, NHTCU places roughly 10 staff members with digital expertise in each of the larger cities (i.e. Amsterdam, Den Haag and Rotterdam), and fewer, if any, in the smaller cities.

As part of a larger evolution in Dutch responses to cybercrime, the NHTCU has had its budget tripled between 2011 and 2012, and is looking to increase the number of full-time staff it currently employs.

Processes

NHTCU teams work on cases which are (1) high impact, (2) organised and targeted at the national infrastructure, and (3) innovative. Typically, the unit runs approximately four major projects each lasting six months. The unit is also responsible for all instances of mutual legal assistance (MLAs), provides forensics support and offers training to stakeholders on technical matters and IT literacy.

Currently, it collaborates with the private sector on an experimental basis. The unit hosts 10 private-sector staff under secondment; leadership within the organisation acknowledges the importance of private-sector collaboration for future development. The unit also collaborates tentatively with the EUCTF. NHTCU collaboration with Europol and Interpol is conducted via the International Police liaison (Interpol). The unit interacts with AWF Cyborg on only a limited basis.

Outputs

Following the Bredolab botnet project, no phishing attacks were launched against Dutch banks for 18 months. Officials within the organisation estimate its impact to be limited in terms of prosecution but far higher in regards to deterrence through the publication of information.

Outcomes

A number of structural challenges affect NHCTU operations. The unit's regional and local-level work lags behind its national activities, as cybercrime is largely not yet prioritised at the regional level. Recently, this has been mitigated by greater co-ordinated efforts on the part of local and regional forces to address particular aspects of cybercrime. Since NHCTU projects tend to be short-term, there also exists a need to create a system to ensure that issues continue to be addressed once the initial intervention has abated.

Another significant challenge lies in incentivising information-sharing between cybercrime units. This is particularly the case in regard to Cyborg, which is currently thought to be of little benefit to NHCTU operations owing to the cumbersome nature of its information-disclosure mechanisms. Until these challenges are addressed, personalised contacts are likely to continue to play a significant role in information-sharing and co-operation.

Poland – Wydział Wparcia Zwalczania Cyberprzestepczosci (Unit to support the fight against cybercrime) Criminal Bureau of Investigation, General Headquarters of Police

Context:

Poland confronts similar cybercrime issues as the other EU Member States. Internet penetration in the country occurred very rapidly, growing from 5,000 users in 1990 to 16 million today. The country's Police Act of 1990 addresses the relationship of the penal code to information and telecommunication systems. Compared to other countries, Poland is considered very liberal, as police do not need to obtain a court order when requesting information from ISPs for operational work. They may also retain data for 24 months.

Poland is in the midst of restructuring its response to cybercrime. A particular organisation deals with cybercrime threats to critical infrastructure, while different elements within the police have cybercrime units. The cybercrime unit sits within the National Police headquarters and reports to the Ministry of the Interior.

The cybercrime unit consists of three teams. The first, dedicated to threats analysis, runs undercover investigations on the Internet. The second addresses technical support and computer forensics, while the third works on international co-operation.

Input

The unit employs 23 full time staff members, eight of whom work on the threats analysis team, six on technical support and nine on international co-operation. All employees are police officers, but with specialist expertise.

Processes

The Criminal Bureau of Investigation deals with tackling cybercrime, while online economic fraud is dealt with by the Anti-Fraud Department. The remainder is handled by the cybercrime support unit. Activities often overlap between units, for example child pornography being addressed by both the child abuse unit and the cybercrime unit. The unit also works to prevent the sale of stolen goods on websites in Poland and to counter the threat of online harassment.

The department's role is largely operational. It is involved in collecting evidence and initiating investigations. It also conducts training for other departments and police officers on how to address cybercrime and runs information and prevention campaigns as part of its outreach activities.

The unit co-operates with Europol to receive training and information about Polish Internet users. It does not participate in Cyborg because of the latter's bureaucratic inefficiencies and slow timescales.

Output

The unit does not collect its own statistics. Statistics are instead collected by the police as a whole. These address trends of criminal activity and determine an appropriate threat and resourcing level.

Outcomes and impact

Officials within the Polish cybercrime unit believe the ECC might provide European training regarding cybercrime and best practices. It might also reduce bureaucracy and enable faster information-sharing between Member States.

Romania – Romanian Cybercrime Unit

Context

The Romanian Cybercrime Unit was created in 2003 as part of the Directorate for Countering Organised Criminality of the General Inspectorate of Police. It sits within this Directorate alongside units dedicated to terrorist financing, money laundering and drugs. This structure is mirrored on the legal side by the general prosecutor's office, with whom it works quite closely.

The unit consists of two sections dedicated to investigation and forensics respectively, and is split between a central headquarters and 42 smaller cyber units and brigades spread throughout the field offices.

Romanian law states that anyone with knowledge of a crime must report it, but in practice there is little incentive to do so. The cybercrime response is further complicated by the fact that victims of fraud frequently live outside of Romania, either in the rest of Europe or in the USA.

Input

Cybercrime capability in Romania is made up of 198 people, 28 of whom are based at the headquarters in Bucharest. The central unit employs 18 people in its investigative section and 10 in its forensics section. Only the head of the overall unit and the two section leaders take part in non-investigative activities. Individuals throughout the unit tend to fulfil a variety of roles, though one person in each county is specifically responsible for handling child pornography. Most staff members are drawn from the police academy and have a background in law and IT. Further training, facilitated by Europol and the private sector, is completed once employees join the unit.

Processes

The central unit's primary functions include co-ordinating the independent investigations of the field offices, and running investigations that involve operations in Bucharest or that involve cross-county or cross-border dimensions. It also co-ordinates with prosecutors, conducts activity evaluations, and provides digital forensics and forensics support for other police units.

In contrast, the field offices are primarily responsible for conducting local investigations and for co-operating with local governmental agencies and the private sector. A smaller forensics capability is also distributed throughout the counties.

The cybercrime unit runs a website (@frauds.ro) that allows individuals to report incidences of cybercrime. It is also a useful preventative tool.

The unit collaborates with the private sector and international organisations such as Europol. It contributes to AWF Cyborg, Twins and Terminal. Nonetheless, officials believe its most fruitful interactions are the bilateral exchanges that take place with other states.

Output

A large amount of Romanian cybercrime affects individuals outside of the country's borders. This in turn affects the ability of law enforcement to estimate the levels of cybercrime and the impacts of their efforts within the country. The unit estimates that it is aware of 60–70 percent of cross-border cybercrime and 90–95 percent of the cybercrime that occurs within Romania.

The unit produces monthly reports on its activities. In the first half of 2011, the unit had four take-downs for major cases, which involved the issuing of 30 search warrants and the charging of 43 individuals; 25 new cases were registered and there were four indictments for major cases.

Outcomes and impact

Most of the unit's investigations are finalised, though cases are sometimes stalled because of difficulties in co-operation with other countries. Within Romania, an increasing number of cybercrime cases are being reported and solved.

Slovenia – Computer Investigation Centre, Criminal Police Directorate

Context

Slovenia defines computer crime strictly as involving the intrusion and misuse of personal data. Changes in the country's procedural law in October 2009 introduced new types of offences to the criminal code. The two new articles included provisions on how to handle seized equipment, how to handle data, and what to include in reports. They also allow for suspects to be present during the acquisition of evidence. Slovenia's high levels of data privacy require court orders for many police actions.

The Slovenian cybercrime unit within the Slovenian police was established in April 2009 after three years of development. The unit was originally housed within the financial crimes division, but now sits independently alongside other units. Roughly 80 percent of the department's capacity is engaged in assisting other police units with computer forensics, while the remainder is dedicated to tackling cybercrime relating to attacks against information systems and data. The unit is particularly active in regard to private-sector security needs, but overall its work is largely reactive and in response to reported cases.

Input

Currently the cybercrime unit employs 45 people, five of whom are based in the unit's headquarters and the remainder of whom are distributed throughout the country's 11 police directorates. Most members of staff are police officers, but there are also some employees from the private sector involved in networking, mail and web servers, and programming. Each unit within the Slovene police force is allocated the same budget, however given the high priority status of the cybercrime section, it has no difficulty making additional budget requests.

Processes

The unit performs substantial amounts of training, particularly in support of the regional police departments. It can also arrange specialised courses should the need arise. The unit also does some R&D, particularly in the areas of malware analysis and software training.

The department's other main areas of activity are computer forensics and investigation. Since the cybercrime unit was first established, there has been a significant increase in the volume of computer forensics it performs. This is driven by growth in the unit's staff and by an increased awareness of other parts of the police of the cybercrime unit's capabilities.

The department also runs an anonymous telephone hotline through which members of the public can report instances of corruption, child pornography, and the like. Victims of cybercrime can also report crimes directly to the unit.

Currently, the unit conducts most of its collaboration informally. It is working to establish more formal channels of co-operation with ISPs and other private-sector companies involved in IT security, such as the Slovenian CERT. Slovenia does not yet contribute to AWF Cyborg, but its cybercrime unit in Mariposa engages in regional collaboration with Bosnia and Croatia, and also internationally with organisations such as the FBI and

Spanish law enforcement. Slovenia is also part of the Council of Europe project on Cybercrime IPA.

Output

The cybercrime unit uses the central police database and statistics to monitor its performance. There are no legal requirements to report data to any centralised unit.

Outcomes and impact

Poor levels of feedback from prosecutors impede the unit's understanding of outcomes. Generally, judges and prosecutors do not always understand IT or cybercrime, and thus may have difficulty working with the evidence processed by the unit.

Spain – High-Tech Crime Unit, National Police

Context

Spain first created a group to investigate high-tech crime in 1996. In 2002, the High-tech Crime Unit was officially established as part of the Criminality Unit within the National Police. The National Police have a presence in all 17 major Spanish cities and are responsible for handling drugs, immigration, documentation, and international co-operation. They frequently work with the Guardia Civil, a more regional law enforcement body, in smaller cities and towns.

In addition to its Criminality Unit, the National Police also contains sections dedicated to terrorism, forensics, immigration, and the uniformed police. HTCU's mandate stems from the power of the Director of the Crime Division to create units and sections within the National Police as is deemed necessary.

HTCU is itself composed of four main divisions. The first of these addresses crimes against persons, including pornography, child abuse, and social network harassment. The second deals with economic crimes, including fraud, phishing and intellectual property. The third division is dedicated to anti-piracy, while the fourth fulfils a support function in forensic software analysis, training, and interfacing with the private sector.

Input

The central Unit staffs 46 full time employees, all of whom are required to be police officers. Regional and city units have on average eight full-time staff members each, though Madrid, with 20, has far more. Regional staff members are not solely dedicated to cybercrime, however, and also work on broader economic crimes. Budgetary decisions fall to the General Director for the criminal police.

Processes

HTCU's main activities involve investigations and prosecution. The unit also organises two-week training courses for officers and investigators in other sections of the National Police, with the intent of enabling participants to conduct simple cybercrime investigations. They also provide joint training with the Guardia Civil for senior officers. These sessions are aimed at addressing more complicated instances of cybercrime.

HCTU conducts limited ad hoc R&D, collaborating especially with the private sector and international groups such as ECTEG and the EUCTF. This research is intended to develop tools for investigation, a common training programme, and further training materials. The unit's outreach efforts are conducted via a Facebook and tuenti (Spanish social media) page, conferences at universities and foundations, and its own webpage. The unit also runs an outreach programme in Spanish schools as part of a joint effort with Microsoft.

Currently, the unit does not collate or produce intelligence or conduct its own forensics analysis. These needs are met by other units within the National Police. Analysts based in the HTCU use information from the central intelligence unit's database. The technical section of the national police also provides forensics capabilities to the HTCU. They have staff dedicated to forensics analysis and reporting for internal purposes as well as for getting warrants and facilitating prosecution. Within the HTCU, there are also technical specialists who prepare forensic evidence for use in court.

The unit collaborates productively with NGOs, the private sector, the Guardia Civil, Interpol and Europol. Collaboration depends on the area of investigation, with child protection involving partnering with NGOs and hacking primarily involving partnership with private sector companies in the development of anti-virus software. Collaboration with Europol and Interpol is particularly useful in enhancing data on child abuse and botnets, where as collaboration with Spain's CERT has been particularly fruitful in advancing investigations involving malware and malicious code.

Output

HTCU conducts more than 1,000 prosecutions per year, with a success rate of greater than 50 percent. The unit's work contributes to the overall targets and performance of the Criminal Division of the National Police, but no specific numerical targets are set for HTCU activities.

Outcomes and impact

HCTU is well known in Spain to members of the public and criminals alike. Evidence suggests that the latter are moving to locations or networks that are less-well policed, as fewer Spanish ISPs are being used for criminal purposes. In respect to child pornography, for example, cybercriminals have moved from P2P to more sophisticated networks.

Currently, Spanish attempts at collaboration are sometimes impeded by national and international bureaucratic procedures or by the limited operational capacity of certain institutions. National legislation also imposes procedural requirements on collaboration that prevent the occurrence of informal co-operation within a sufficiently short timescale. It is expected that collaboration with the future ECC will be significant because of the Centre's greater information- and contact-sharing capacities and its ability to provide access to different providers, such as private-sector stakeholders.

Sweden – National Bureau of Investigation

Context

Sweden's police force is highly centralised, with one police organisation headed by the chief of the National Board. The force is composed of a Forensics Lab, Security Services, and the National Bureau of Investigation. There are also 21 local policy authorities responsible for combating crime in their respective areas. The central unit deals with serious organised crime and crime with international dimensions.

The National IT Crime Unit was established in 1986 and sits within the Bureau of Investigation. The unit is made up of three groups: a forensics team, a child protection unit, and an Internet unit. The organisation does not have a special mandate, and most of its work involves supporting other sections of the police in their investigations.

Input

The IT Crime Unit employs about 30 people, all of whom are police officers except for the administrative staff and two technicians. Applicants to the department must have experience in investigation and an interest in IT. The unit operates on a budget of €2.5 million.

Processes

The IT Crime Unit primarily assists other police departments in their investigations. They also advise and provide training for prosecutors. The unit has no intelligence function or dedicated analysts on staff. One staff member feeds data into Cyborg.

Forensics constitutes another important area of activity. The unit handles forensics on computers, GPS devices, telephones and cameras, and its police officers all have training in digital forensics. Forensics labs conduct research and development for IT and IT crime, while academic IT specialists at the National Forensics Lab provide further training.

The unit conducts collaboration at many levels, both within and outside of the police. External partners include the Swedish military, ISPs, universities and other organisations. University collaboration tends to focus on finding solutions to specialised technical problems.

Additionally, the unit participates in Interpol's Working Party on High-Tech Crime and its child pornography group is represented in several international organisations. Officials within the IT crime unit also consider Europol a particularly important partner.

Output

Given the unit's primarily supportive role, it receives little feedback and metrics of its own.

Outcomes and impact

Feedback from other units within the Swedish police suggests that practices such as Internet wiretappings have helped move investigations forward. Recently, the IT team was particularly involved in a case of a helicopter stolen in September 2009, for which 15 people were ultimately prosecuted and convicted.

Given that the Data Retention Directive has yet to be implemented in Sweden, ISP logs are cleared after just three months. This hinders co-operation with international partners and limits the unit's capabilities within Sweden. The international dimension of cybercrime continues to challenge law enforcement in the country, as Swedish customers use foreign, and particularly American, services.

United Kingdom – Cyber; Serious and Organised Crime Agency (SOCA)

Context

The UK's Serious and Organised Crime Agency (SOCA) was formed in 2006 by the Blair government. It was the product of a merger between the National Crime Squad, the Criminal Intelligence Service, those sections of Customs and Revenue in charge of drugs, and portions of the immigration service. Unlike its predecessors, it has a strategic harm-reduction approach.

As of August 2011, the intention is to rebrand SOCA and bring it under the umbrella of the yet-to-be-founded National Crime Agency. This agency will have four pillars dedicated, in turn, to organised crime, the UK Border Authority, an economic crime agency, and CEOP. In addition to these pillars, there will be cross-agency functions that include intelligence, corporate functions, and a National Cybercrime Centre (NCC). The NCC is intended as an operational unit, but it will also support the other four pillars.

Simultaneously, SOCA is today undergoing a reorganisation as a result of lessons learned from its first five years in operation. The reorganised unit will focus on traditional organised crime facilitated through the Internet, as well as phishing and economic crime. It will be organised around a new "SOCA operations centre."

The current SOCA is mandated directly by the Home Secretary to: build knowledge and understanding of organised crime; develop an intelligence picture of organised crime; tackle financial crime and criminal finances; raise the risks for criminals; and work internationally. Generally, SOCA addresses the non-fiscal aspects of cybercrime and the organised criminal elements of cybercrime. The National Fraud Agency currently handles the financial aspects of cybercrime, while the Department for Business, Innovation and Skills addresses intellectual property issues. The London Metropolitan Police also have an e-crime Unit (PeCU) that addresses cybercrimes that affect London.

Inputs

SOCA maintains officers in roughly 50 countries. Currently, the cybercrime department operates on an annual budget of roughly €3.3 million (£2.9 million) and has 104 full-time employees dedicated to cyber issues. Last year's cybersecurity strategy pushed cybersecurity up to a Tier 1 threat and allocated €757 million (£650 million) to addressing the issue. Of this, €22 million (£19 million) was allocated to SOCA for four years.

Processes

As a result of the organisation's strategic harm-reduction approach, obtaining judicial outcomes is just one aspect of its activities. Disruption and prevention are equally, if not more, important. This approach also enables the organisation to be selective when deciding which cases to investigate. The cybercrime unit undertakes strategic assessed reporting and tactical work and produces thematic reports. It conducts regular operations as well as a number of specialised ad hoc projects which may involve issues such as Internet governance, data breach, and the criminal marketplace.

SOCA's engagement with industry stakeholders is wide ranging and across all sectors. Prevention is a large component of this collaboration, with SOCA providing knowledge and specialised products to the private sector. The unit also engages with the Security Services and is a key stakeholder in the National Cyber Security Programme.

SOCA is also active in regards to international co-operation, through both international co-operative channels and its own network of international offices. The organisation works collaboratively with the Strategic Alliance Group (UK, US, Australia, New Zealand and Canada). It also seeks to influence other countries and change the terms of their modus operandi and objectives. The unit collaborates closely with international units that operate in different regulatory frameworks or with different skill sets, such as the Dutch and German cybercrime units, and organises a world-renowned conference each year. SOCA performs a co-ordination function in regard to Europol and Interpol, but does not have the competence to speak for the United Kingdom in either body.

Output

SOCA measures the number of arrests achieved or assisted by business unit and records its disruptive activities. The cybercrime unit reports to the SOCA Board and ultimately to the Home Secretary. In the absence of an accurate baseline measure, reporting figures on the levels of cybercrime or the unit's impact has proven difficult. The government is addressing this issue by establishing a reporting centre.

Outcomes and impact

SOCA's approach and operational model has gained great traction and garnered much enthusiasm, both within the UK and abroad. The tangible impact of the cybercrime unit is less obvious, especially given the fact that much of the infrastructure involved in its investigations is based in America. International co-operation and collaboration with organisations such as Europol or the potential ECC continues to be complicated by the different priorities, interests, agendas, and systems of participating countries.

Appendix D: Analysis of data on recorded cybercrime offences across several European countries

In this appendix we plot data from the European Sourcebook on Crime and Criminal Justice statistics to illustrate the correlation between recorded offences and percentage population online.

From the European Sourcebook we plot number of recorded offences, per 100,000 people relating to computer crimes against data, systems.[48]

According to the standard definition given in the European Sourcebook, “offences against the confidentiality, integrity and availability of computer data and systems” comprise unauthorised entry into electronic systems (computers) or unauthorised use or manipulation of electronic systems, data or software. Where possible, the figures include:

Illegal access (i.e. intentional access to a computer system without right, e.g. “hacking”).

- Illegal interception (i.e. interception without right, made by technical means, of non-public transmissions of computer data).
- Data interference (i.e. damaging, deletion, deterioration, alteration or suppression of computer data without right).
- System interference (i.e. serious hindering without right of the functioning of a computer system).
- Misuse of devices (i.e. production, sale, procurement for use, import, or distribution of a device or a computer password/access code).
- Computer fraud (i.e. deception of a computer instead of a human being).
- Attempts at any of the above.

but exclude:

- Illegal downloading of data or programs.

[48] http://europeansourcebook.org/ob285_full.pdf

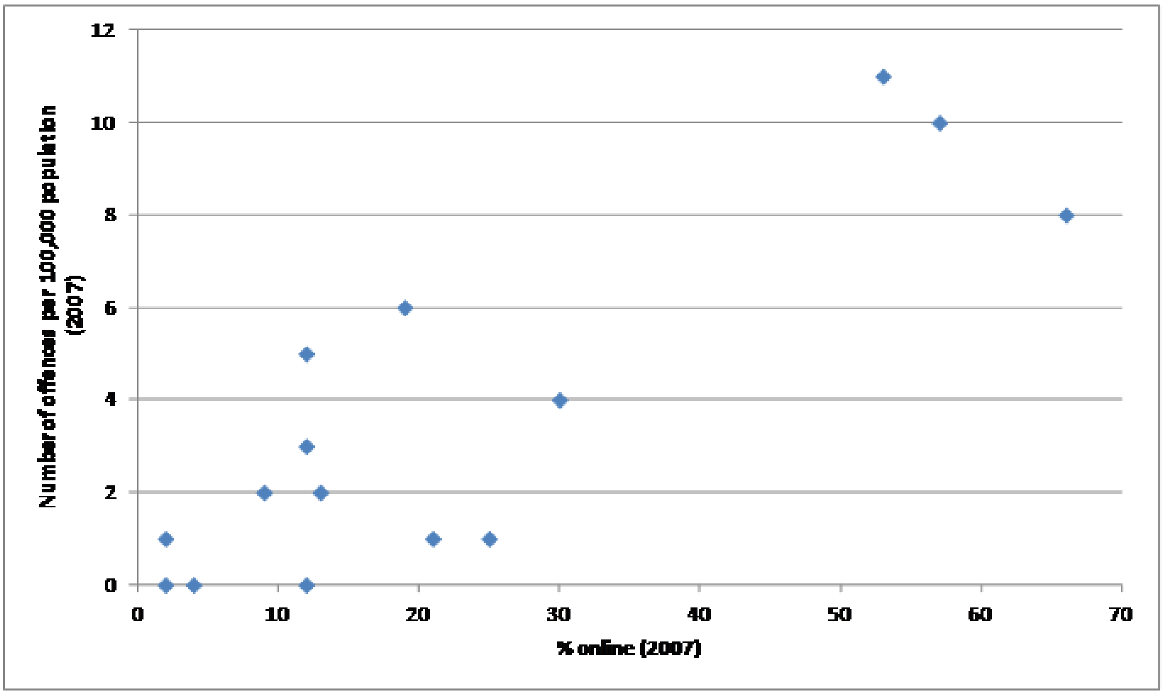
Table D.1 European Sourcebook: Cybercrime Statistics

	2003	2004	2005	2006	2007
Albania					0
Armenia	0	0	0	0	0
Austria	2	2	3	4	4
Belgium	14	49	42	53	
Bosnia-Herzegovina					
Bulgaria	0	0	0	0	0
Croatia	0	0	0	1	2
Cyprus				1	3
Czech Republic	0	0	0	0	0
Denmark	9	7	11	11	
Estonia	2	3	4	7	11
Finland	11	6	6	7	8
France					
Georgia					
Germany	69	76	70	66	67
Greece					
Hungary	7	10	5	5	5
Iceland	0	0	0	0	
Ireland	0	0	0	0	1
Italy		2	3	4	
Latvia				1	
Lithuania	11	0	1	1	1
Luxembourg					
Malta					
Moldova	1	0	0	0	0
Netherlands					
Norway					
Poland	1	1	2	2	2
Portugal	1	2	3	5	
Romania	0	0	0	2	1
Russia	5	6	7	6	5
Slovakia					
Slovenia	1	2	3	2	6
Spain					
Sweden	8	8	7	9	10
Switzerland					
TFYR of Macedonia					

Turkey				0	0
Ukraine	0	0	0	0	0
UK: England & Wales					
UK: Northern Ireland					
UK: Scotland					
Mean	6	8	7	7	6
Median	1	2	3	2	2
Minimum	0	0	0	0	0
Maximum	69	76	70	66	67
Total	*142*	*174*	*167*	*187*	*126*

As can be seen (for example with France) there are gaps in the data. We see something of a correlation between this data for 2007 and number of people online in each country – that is to say, there is some kind of relationship between the number of people online and the extent of recorded offences. This is presented below. Note that this excludes Germany as an outlier.

Figure D.1 Assessment of the relationship between reported cybercrime and Internet penetration



Appendix E: Examples of co-operation

We describe examples of co-operation relevant to the domain of cybercrime below by way of informing the operation of the co-operation and co-ordination activities of the ECC.

2CENTRE – Cybercrime Centres of Excellence Network for Training Research and Education[49]

'2CENTRE' is a major two year project funded by the European Commission. Its purpose is to create a European network of Cybercrime Centres of Excellence for Training, Research and Education. Two national centres have already been established, one in Ireland and one in France. Total project funding was €3million.[50]

Each national centre will be a partnership between law enforcement, industry and academia. The partners will work together to develop a range of activities, including training programmes and qualifications for both LE and non-LE cybercrime professionals, quality research products, and tools for use in the fight against cybercrime.

A 2CENTRE Network Coordination Centre will be created to encourage excellence, relationship building, network expansion and links to international bodies. New members will be encouraged to join the network during the project and support will be provided to enable this. Once the project is completed, in 2013, there will be a sustainable network that will continue to grow in future years to create a truly global collaborative platform.

The 2CENTRE EC project comprises of

- a Network Coordination node
- a Centre of Excellence in Ireland (University College Dublin, CCI)
- a Centre of Excellence in France (Universities of Troyes and Montpellier 1)

2-CENTRE in France

According to a 2011 press release[51], €980,000 was allocated to the 2-CENTRE in France. The partners in the French 2-CENTRE are:

- Université de Technologie de Troyes

[49] http://cci.ucd.ie/content/2centre-1

[50] http://ccicybercon.org/2centre

[51] Fn to French set up

- Université de Montpellier 1
- Thales Communications SA
- Gendarmerie Nationale
- Police Nationale
- Microsoft France
- France Orange

2-CENTRE in Ireland

Partners to the 2-CENTRE in Ireland are:

- An Garda Siochana
- Microsoft (Ireland)
- Microsoft Corporation
- Aconite Internet Solutions Ltd.
- Irish Banking Federation
- INFACT
- eBay

B-CCENTRE – Belgian Cybercrime Centre of Excellence for Training, Research and Education

In 2011 the B-CCENTRE was established.[52] The B-CCENTRE aims to be the main platform for collaboration and coordination with regard to cybercrime matters in Belgium, combining expertise of academic research groups, industry players and public organisations (law enforcement, judges and policymakers). B-CCENTRE conducts interdisciplinary fundamental research in technology, ICT and Media law, criminal law and criminology as well as basic and advanced ICT and cybercrime training and awareness related issues for law enforcement professionals and public and private sector (e.g. judges, lawyers, businesses).

In addition, B-CCENTRE is intended to become a platform for national and international collaboration across different actors involved in tackling cybercrime; co-ordination of existing expertise and driving a co-ordinated policy approach. The B-CCENTRE also hopes to co-ordinate and collaborate within other organisations such as the UVT and WODC in the Netherlands and with the 2CENTRE network (although B-CCENTRE is not at present part of the 2CENTRE). It is understood that the B-CCENTRE has 10 full time researchers and is hosted at K.U. Leuven.

Reitox Network / RTX Unit in the EMCDDA

One possible model to implement co-operation under the remit of the ECC might be the Reitox and International Co-operation unit of the ECMDDA. Its mission and functions are described below in Table E.1 below. As can be seen, the Reitox unit performs similar

[52] http://www.b-ccentre.be/[52] As of 15 February 2012: http://www.b-ccentre.be/

tasks, at a similar level of magnitude – i.e. at a pan European level) as might be expected for an ECC.

Table E.1: - Mission, function and activities of the RTX unit of the ECMDDA

Unit	Mission	Activities
Reitox and international cooperation (RTX) unit	The main role of the Reitox and international cooperation unit is to coordinate a network of National focal points (NFPs), set up in the 27 EU Member States, Norway, the European Commission and in the candidate countries. Together, these information collection and exchange points form Reitox, the European information network on drugs and drug addiction.	• to assist the scientific departments of the EMCDDA in coordinating the collection of the data in all Member States through the Reitox National focal points; • to assist the National focal points in their active participation in the EMCDDA work programmes, namely the implementation of the key indicators and other core data, at national level, and in the production of their national reporting (national report, standard tables and structured questionnaires); • to promote the Reitox-based model for data collection on drugs in Europe.

Source: EMCDDA website

According to the 2012 EMCDDA work programme, the RTX unit has 14 posts allocated to this unit. This includes 5 on the Reitox European co-ordination team and the remainder on international co-operation.

Other models of co-operation

Other models of co-operation and collaboration might well be instructive to consider. At the Member State level, for example, KLPD, BKA and SOCA all have models of co-operation where law enforcement and the private sector physically are co-located to work on common cases. At the European level, the EP3R (European Public Private Partnership for Resilience) also exists which brings together public and private sectors to discuss issues concerning resilience. ENISA plays a role in EP3R. Other pan European models for co-operation include the European Judicial Network (EJN) and the European Genocide Network (EGN) both of which use Eurojust as a platform to facilitate and support co-ordination and co-operation between judicial authorities across the European Union.

Appendix F: Cost Estimates for a European Cybercrime Centre

The following tables break down the costs summarised in Chapters 8 and 9 of this report concerning capital and operating expenditure for the ECC under different options.

Estimating resources is a complex task fraught with uncertainty and thus we provide broad point indications that are deterministic and not probabilistic.

In the cost estimation exercise for an ECC, we use a range of approaches, including taking data reported to us by stakeholders in the study, extrapolating from other relevant but recent data and using comparable proxies (where similar activities are being done in other domains that share some characteristics of the costs we are trying to estimate). This is particularly the case where we have used the European Monitoring Centre for Drugs and Drug Addiction (EMCDDA) as a proxy to inform consideration of the number of posts required for co-ordination activities with the national CERT–LEA Focal Points. The domain of drugs and drug addiction shares enough similar characteristics to cybercrime to make it a useful proxy. Such characteristics include expert opinion about the difference between the reported and actual figures, the trans-border nature of the phenomena and its complexity.

Other analogies include reference to the secretariats of the European Justice Network (EJN) and European Genocide Network (EGN), currently run by Eurojust. We extrapolate the patterns of posts dedicated to criminal intelligence analysis of different types of cybercrime in Europol based on the numbers of personnel Europol have currently reported as working on cybercrime. We also estimate following the pattern of posts based on indications reported to us by Europol on 20 October 2011.[53] We extrapolate to determine the likely workload for a possible reporting centre and for a number of other costs (for example, training). Throughout, we draw on expert opinion using data from the interviews and workshops with the stakeholders consulted so far in the study.

[53] Personal communication from Victoria Baines (Strategic Analyst, Europol) 20 December 2011 based on Europol File no. 2720–29 (2011). This figure is informed by Europol's own expert opinion and views on the scale of the phenomena from access to Restricted criminal justice data (e.g. criminal intelligence stored in the AWFs).

Table F.1 below indicates the sources for our data.

Table F.1 Sources for cost estimates

Item	Source	Reference	Remarks
Personnel costs	European Commission, DG Budget: Budgetary fiche 2008, inflated for 2011 prices	Note de l'unite BUDG/A5 du 15/09/2008 ref MM D(2008)58297 Note a l'attention de des Chefs d'unites responsables de ressources humaines et/ou financiers Bruxelles le 13 octobre 2008	Adjusted for 2011
Desktop IT costs	Europol	Summary for RAND Europe and DG HOME of Europol Costing Exercises for the European Cybercrime Centre (ECC) (File no. 2720–29 The Hague, 20 October 2011)	
Cost of IT infrastructure	Europol	Summary for RAND Europe and DG HOME of Europol Costing Exercises for the European Cybercrime Centre (ECC) (File no. 2720–29 The Hague, 20 October 2011)	
Training	ECTEG Budget under the Programme on Prevention of and Fight Against Crime (ISEC Programme)	E-mail from European Commission DG HOME 21/10/2011 "ECC Cost Estimate – Training"	
Training	Europol	Presentation given by Nicole Di Leone to Co-operation against cybercrime conference 23–25 March 2010. As of 20 February 2012: http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/cy-activity-Interface-2010/Presentations/default_en.asp	
Travel and subsistence costs (per person)	ECTEG Budget under the Programme on Prevention of and Fight Against Crime (ISEC Programme)	E-mail from European Commission 21/10/2011 "ECC Cost Estimate – Training"	
Translation	CEPOL Budget 2011	CEPOL – Budget 2011 Annex. As of 20 February 2012: http://www.cepol.europa.eu/fileadmin/	

		website/newsroom/pubblications/Annual_Budget_2011.pdf	
Studies, research and good practice	CEPOL Budget 2011; ENISA;	CEPOL – Budget 2011 Annex. As of 20 February 2012: http://www.cepol.europa.eu/fileadmin/website/newsroom/pubblications/Annual_Budget_2011.pdf	Based on reported cost for studies and research into cybercrime, in addition to average budget per study from ENISA WP 2011
Events	CEPOL Budget 2011	CEPOL – Budget 2011 Annex. As of 20 February 2012: http://www.cepol.europa.eu/fileadmin/website/newsroom/pubblications/Annual_Budget_2011.pdf	
Publications & communications	RAND Europe	Estimate	Based on internal estimate for publications and communications effort
Data from private sector	RAND Europe	Estimate	
Co-funding for Joint LEA–PPP Network	Standard co-funding threshold under EU Grant support for FP7/Horizon 2020 Programme	As of 20 February 2012: http://cordis.europa.eu/fp7/understand_en.html	
Standards based technical platform for sharing and reporting of cybercrime	European Commission	European Commission	Study to estimate the impact of a pan-European System for the Monitoring and Surveillance of Substances of Human Origin (SoHO)
Training and security accreditation for new personnel at EHQ	RAND Europe	Estimate	Estimate
Programme Risk	Mott Macdonald Review of Large Public Procurement in the UK 2002	As of 20 February 2012: http://www.parliament.vic.gov.au/images/stories/committees/paec/2010-11_Budget_Estimates/Extra_bits/Mott_McDonald_Flyvberg_Blake_Dawson_Waldron_studies.pdf	

In the presentation of all our data in the main body of the report, we round to either the nearest million or nearest hundred-thousand Euro to maximise accessibility and reflect the degree of precision with we wish to accord these estimates. We split attribution of cost implications into two main areas:

- One-off costs – for example the purchase of new equipment, the commissioning of a software platform or acquisition of books, materials or design or one-off strategic advice.
- Ongoing costs – includes a variety of types of cost that might occur on an ongoing basis. The prime example here is staffing. Other examples include consumables for ICT systems and services such as translation for which an annual charge may be necessary). Other types of operating expenditure include the yearly rent or charges for the use of infrastructure (which effectively may bundle up many different types of operating expenditure costs into one simple figure).

The kinds of resource costs that might be of relevance to the ECC include non-infrastructure-related capital expenditure (e.g. design and engineering personnel for a specific project or development of an ICT application) and varying types of operating expenditure (staff costs, service-level agreement charges, ICT consumables, annual payments, etc.).

The reason we do not cover significant capital infrastructure expenditure is that each option considered as feasible does not require new buildings or the acquisition of extensive ICT infrastructure. Each option includes the involvement of Europol in some way, which permits significant synergies with regard to exploiting capital expenditure.

There is already significant investment in a number of information technology resources made by Europol. This includes the Data Centre, the Europol Information System and extended Computer Forensic Network (CFN) as well as the Secure Information Exchange Networking Application (SIENA) infrastructure allowing Member States to transmit and receive messages to the Europol Information System (EIS) and AWFs. In addition, the new Europol HQ has recently opened (at an reported cost of ~€25 million) in the Netherlands. This has specialised space for forensic activities (e.g. anti-static flooring) and guarding, support (e.g. catering staff) and other personnel through which it might be possible to achieve synergies were the ECC physically located there.

One-off costs

We begin by describing one off costs. Table F.2 presents these one-off costs.

Table F.2 General one-off costs

No.		Explanation	Cost p.a. (€)
1	Desktop ICT equipment	Secured and accredited desktop infrastructure per staff member suitable to be used in EHQ	4000
2	Syllabus update	One off cost of reviewing and updating the training syllabus for all members of the criminal justice community	200,000
3	Requirements gathering	One-off costs to commission an IT contractor to collect requirements from all stakeholders for a standards based online reporting and information exchange tool	200,000
4	Software development	One off costs for an public, private or NGO-based software engineering team to design, develop, test and implement a standards based online reporting and information exchange tool	133,000–267,000

Capital expenditure involved in designing, developing and testing an online reporting software application tool

We assume that the only capital expenditure required for this would be an application development team to conduct requirements analysis, design, develop, test and deploy an online reporting application using the aforementioned standard. No additional infrastructure costs would be required since this would be hosted on Europol's own Data Centre on behalf of a Member State or provided as a downloadable software application for installation and deployment on Member State own infrastructure. A summary is provided below at Table F.3.

Table F.3 Capital and operating expenditure for the design, development, testing of a standards based online reporting tool

Type of Expenditure	Cost (EU official) (€)	Cost (private sector) (€)	Cost (NGO) (€)
Capital Expenditure	223,000	267,000	133,000

Ongoing costs

Next, we turn to ongoing costs, which, as we have seen, are chiefly made up of those associated with personnel, service charges, various costs associated with governance (e.g. travel and subsistence), funding and so on.

Inputs to estimate costs of personnel

It is necessary to understand the different types of staff profile likely to involve an ECC and also how the different activities affect different staffing requirements. Our evidence-gathering identified posts that were employed to perform specific activities associated with either criminal intelligence or operational support to Member State investigations. These were known as Restricted posts. We assume that other posts which might be Unrestricted (and therefore could be filled by seconded national experts or contractors) include those doing training or best practice development or outreach activities or other support roles (such as managerial staff, communications, administrators, etc.).

Furthermore we assume that Restricted posts are more closely correlated to the workload of the number of cybercrime cases that could be run than, for example, posts undertaking governance or co-operation activities. Regardless of how many investigations the ECC might run, a Head, Programme Manager and administrative support would still be required. This is also the case for activities concerning co-operation and collaboration (noting the previously referenced EMCDDA proxy).

In order to estimate how much it would cost per year to employ staff we used data from an Internal EU Services 2008 budget Memo[54] concerning the financial implication of different posts for budgetary planning purposes. We adjusted these figures to reflect the likely implication for 2011 by compensating for inflation since 2008. We used a Consumer Price Index for inflation of 1.9 percent per year. The figures represent the “fully loaded” cost to employ one Full Time Equivalent (FTE) post – that is to say, costs to a budget line including the employee’s salary, pensions, social security, and other benefits of a post. Note that these reflect an “average” costs per staff member (understood to be taken at the B2 grade). These are described in Table F.4 below.

[54] EU Services (2008)

Table F.4: Full Time Equivalent rounded cost p.a. for different types of staff

No.	Type listed	Explanation	Cost p.a. (€)
1	Cost for EU officials (2008)	Per annum cost for a full EU official	131,540
2	Cost for temporary agent (EU)	Per annum cost to employ a temporary agent on behalf of the EU	131,540
3	Cost for attached national expert	Per annum cost to employ an attached national expert	78,700
4	Cost for contractual agent	Per annum cost to employ a contractual agent	69,000

Understanding the current status quo

We present below the posts currently understood (at the time of preparation of this phase of our study in October 2011) to be working on functional cybercrime-related activities in each of the four main EU institutions discussed during this study.[55] This data was taken from interviews and input where numbers were reported and interaction with relevant stakeholders during the project. Current estimates are based on an assumption that reported data from the stakeholder is accurate. For some organisations (described in the notes below) the set-up of the institution makes it difficult to pinpoint exactly how many posts are working on cybercrime-related activities – therefore we have indicated from the core we witnessed and described further in the cost estimates where this aspect would become relevant. This is particularly the case with Eurojust, where although there are individuals reporting as consultants or Points of Contact for cybercrime, in reality the structure and operating mechanism of the organisation means that those who would deal in cybercrime would be a much larger number, but would not be doing this as a core activity (since they would be covering other forms of criminal activity).

[55] We do not include ECTEG in this listing since it is run as a separate project on a volunteer basis and we include it under considerations for training costs.

TableF.5 Numbers of functional staff involved in different relevant organisations as at June 2011

	Organisation	# posts	Functions
1	Europol	23	Intelligence; investigative support; forensics;
2	Eurojust(1)	3	Internal advice and consultancy on cybercrime
3	ENISA	3(2)	Policy on CERT relations with law enforcement
4	Cepol(3)	3	Facilitating or managing training delivery platforms (both courses and e-learning environments)

Notes:

(1) Noting that due to the unique set up of Eurojust, each national representative may work on cybercrime related cases, but not exclusively. However, in our interactions we consistently observed three individuals participating and self-reporting as being points of contact for cybercrime.

(2) ENISA reported that three posts work (not necessarily all the time) on aspects relating to cybercrime

(3) As with Eurojust, we consistently observed that three individuals participated in the meetings and interactions and self-reported as being concerned with activities relating to cybercrime, however there is no assigned full time expert on cybercrime within CEPOL's 42 personnel but this is not necessarily unusual since the organisation operates as a platform to bring in content experts.

We now turn to what additional personnel would be required to set up and run the ECC.

Personnel for governance of the ECC

We consider that three posts would be necessary to provide for the overall governance and strategic management of the ECC. This would include an ECC Head, a Programme Manager to prepare documentation (e.g. co-operation agreements) and facilitate the work of the Capability Board and an administrative support officer. Table F.6 below sets out the responsibilities of each post.

Table F.6 Overview of responsibilities of ECC governance team

Post	Description of function	# posts
Head	Accountable for delivery of the capability through the ECC, Directs activities of the ECC, executes and signs off on major decisions and Chairs the ECC Capability Board	1
Programme Manager	Responsible for day to day operation of the ECC, drafts agreements and documents	1
Administrative Support Officer	Administrative support for above	1
Total		**3**

It is assumed that due to the high-profile nature of these tasks and the need for the governance team to have insight to be able to interact with Europol restricted posts (particularly with respect to the activities relating to intelligence) these would be EU-level posts.

Personnel for operational investigative support to Member States and criminal intelligence analysis

Table F.7 below indicates additional posts based on a projected hypothetical lower and upper range of additional workload for activities matching Goal 1 (Europol as an EU support centre) and Goal 2 (Europol as an EU Criminal Intelligence Hub) of Europol's current 2012 Work Programme. According to this programme, there were 137 analysts working on Goal 1 and 94 analysts working toward Goal 2. The hypothetical estimates (in italics) were derived from data provided by Europol following internal discussion.[56] The upper estimate constitutes roughly a six-fold increase in personnel from the complement at the time. To provide a lower range, we extrapolate down to a figure reflecting an increase of an additional half as many more personnel (additional 50 percent) as was reported to us as working in the HTCC in June 2011. We employ a pattern-based approach to extrapolate based on the fact that the personnel reported to us were working across both Goals of the Europol 2011 Work Programme. Therefore arrive at the extrapolated figures from taking the ratio of overall Europol personnel working across these two Goals as a means to split personnel into Intelligence but also Operational Support functions, before re-combining. Table F.7 describes the output of this across analysis dealing with all types of cybercrime currently within Europol's cybercrime related mandate.

Table F.7 Range of workload for investigative support and intelligence analysis

	Current posts	Additional posts from current situation	
		Low workload requirement	High workload requirement(1)
Functional personnel (Analysts)	23	*14*	*158*
Supporting personnel	*6*	*7*	*82*
Total		***21***	***240***

(1) based on Europol File no. 2720–29 (2011)

Due to the sensitive (Restricted) nature of these posts, we assume that they can only be performed by a Restricted EU-level post, rendering the resource implication for these activities expensive.

[56] Personal communication from Victoria Baines (Strategic Analyst, Europol) 20 December 2011 based on Europol File no. 2720–29 (2011). This figure is informed by Europol's own expert opinion and views on the scale of the phenomena from access to Restricted criminal justice data (e.g. criminal intelligence stored in the AWFs).

Personnel for co-operation and collaboration activities

Co-operation and collaboration is a mix of personnel and co-funded support from the ECC budget. This is detailed in the table F.8 below (the estimated resource for co-funding is described in the non-labour ongoing resource section).

Table F.8 Resource estimate for co-operation mechanisms of the ECC

	Co-operation mechanism	Type of resource
1	Data Fusion Unit at the ECC	Five posts at the ECC
2	Joint LEA–CERT PPP Network	Co-funding from the ECC to MS (75 percent contribution to one MS-level post alongside the national/governmental CERT)
3	European Cybercrime Resource Facility	Three Posts at the ECC (two professional staff and one administrator as CA)

In Table F.9 below we present the estimated resources required to perform the activities detailed above in respect of co-operation and collaboration.

Table F.9: Resources for co-operation, co-ordination and joint working activities

Area	Posts
Data Fusion Network	5
Joint LEA–CERT PPP Network	n/a
European Cybercrime Resource Facility	3

We base some of our estimates using the EMCDDA Reitox Network model and the RTX Unit (where there are 14 posts, five of which cover the EU and the rest international co-operation) as a proxy. We indicate resource implication whether these posts might be filled as EU-level officials (such as might be the case where these activities take place under the option of an ECC owned by Europol) or as contractual agents or seconded national experts.

The resource implication for the Joint LEA–CERT PPP Network is based on the EMCDDA model where the national focal points were co-funded from the EMCDDA budget.[57]

Finally, the resource implication for the ECRF is based on a calculation of the amount of time it would take to prepare and sign co-operation agreements with 27 different countries (which works out to 1.8 FTE) plus assuming necessary administrative support.

Non-personnel-related ongoing costs

We now turn to consideration of non-personnel-related ongoing costs.

[57] CSES Evaluation Report of the EMCDDA

Cross-cutting resources

For the two options involving an ECC being a separate legal entity we provide for some way that Europol might recover the costs of the necessary use of its expensive capital infrastructure. We portray this as a service charge, governed by the kind of service level agreement common in ICT outsourcing in the private sector. Under this model, we make a basic assumption of dividing a general estimate for the capital costs by 12 to provide the annual service charge for use of the infrastructure. We consider this appropriate to include since in other areas for example large scale IT systems in the area of justice and home affairs) annual charges are payable for connection to the pan-European secured S-TESTA network. These annual service charges applying in the case of the ECC are indicated below in Table F.10.

Table F.10 Example service charges for use of Europol resources by the ECC

Relevant ECC activity	Item	Cost (€)
All	Annualised use of SIENA	166,700.00
All	Annualised use of Data Centre	417,00000
Operational support	Annual use of CFN	250,000
Strategic Intelligence	Annual use of AWF infrastructure	333,000

Non-labour resources for broad-based training, education and best practice development

During the course of our study we identified a number of organisations with an explicit mandate to undertake training, education and exchange of knowledge and information concerning law enforcement aspects of cybercrime in cybercrime related areas. Foremost amongst these was CEPOL and the volunteer-based ECTEG. We extrapolate resource implications from these activities (detailed previously in Chapter 5 and in Chapter 7) using a series of assumptions in order to present a resource estimate for training. We base our resource estimates on an assumption of training supply that is in line with the low/high model indicated for sensitive strategic intelligence and operational support, on the basis that this broadly mirrors the national level activities of law enforcement personnel involved in dealing with cybercrime.

There are costs involved in delivering the training and education courses. This includes time spent lecturing or giving the training and also preparing material. This assumes that no course preparation is required (since ECTEG, CEPOL and others have already developed a syllabus which would need to be updated by the ECC Programme Team). The costs differ depending on whether the course is delivered by an EU-level official (i.e. someone from the ECC, Europol, or Eurojust for example) or a seconded national expert or a contractor.

Table F.11 Costs for delivering a continual professional development programme

	Total	Additional	Additional	Additional
Duration:	Quantity of	cost to	cost to	Cost to

	five-day courses p.a.	deliver using EU agency staff (€)	deliver using attached national expert (€)	deliver using external expert (€)
Current requirements (2009)	3			
Low workload requirement	5	27,500	16,500	14,400
High workload requirement	18	110,100	65,900	57,800

Table F.12 Costs to deliver five-day courses in accredited education programme

Duration:	Total Quantity of five-day courses p.a.	Additional cost to deliver using EU agency staff (€)	Additional cost to deliver using attached national expert (€)	Additional cost to deliver using external expert (€)
Provision (2009)	9	55,000	33,000	28,900
Low workload requirement	14	82,600	49,400	43,300
High workload requirement	54	330,300	197,700	173,300

Table F.13 Costs to deliver ten-day courses in accredited education programme

Duration:	Quantity of ten-day courses p.a.	Additional cost to deliver using EU agency staff (€)	Additional cost to deliver using attached national expert (€)	Additional cost to deliver using External expert (€)
Provision (2009)	2	24,500	14,600	13000
Low workload requirement	3	36,700	22,000	19,200
High workload requirement	12	146,800	88,000	77,000

Using data from the ISEC funding programme, we calculate that the per diem rate for an attendee at a course to be as follows (based on 10 teachers and 30 students) in Table F.14. We also use this sum to estimate general travel and subsistence costs for per person/day in other areas (such as attending the first meeting of the ECC Capability Board.

Table F.14 Estimating travel and subsistence

Item	Costs (€)
Travel & subsistence (40 persons)	1,660,000
Travel & subsistence per person	41,500
Total travel & subsistence (10 teachers)	415,000
Total travel & subsistence (30 students)	1,245,000
Travel & subsistence per day of course	2,000

Source: ECTEG MSc ISEC budget

Other non-labour ongoing resources

Finally, we turn to other costs including travel and subsistence, studies and research, co-funding for the Joint LEA–CERT PPP model, communications, information seminars, data from the private sector, translation and meetings and events and training and security for ECC personnel.

Table F.15 Other ongoing costs

No.		Explanation	Cost p.a. (€)
1	Travel and subsistence	Fee to cover on average one person per day required at ECC-related events or meetings (e.g. annual meeting of the ECC Capability Board; training)	2,000 per person per day required for ECC commitment
2	Co-funding	75% co-funded contribution from the ECC budget to the Joint LEA–CERT PPP network	1,357,000
3	Information seminars	Preparation, management and delivery of information seminars according to the CEPOL model	36,000
4	Data from the private sector	Purchased data-feeds from security service providers in the private sector	10,000
5	Studies and research	Three studies, legal advice or other commissioned consultancy as required	120,000
6	Translation	Translation costs for training and professional development activities	53,000
7	Books & misc.	Provision of books, miscellaneous items	5,000
8	Design and communications	Provision of design support and consultancy for ECC identity and branding	50,000
9	Maintaining the software application	Cost to support the online standards based software platform (e.g. application updates, etc.)	34,000–51,000
9	EHQ training and security	Training and induction for new joiners to EHQ and personnel vetting	300,000

Ongoing costs for maintaining the common reporting platform

Using a proxy for a pan-European monitoring system for bio-vigilance of alerting of Substances of Human Origin (SoHO)[58] where the domain exhibits similar characteristics

[58] See for example the 2010 Impact Assessment of the proposal for a European Single Coding System for Tissues and cells in accordance with Directive 2004/23/EC and European Committee for Standardisation (CEN) Deliverable of CEN/ISSS Workshop on coding and traceability of human tissues and cells, Annex 4:

(namely through the need for a pan-European real-time reporting system using a standards-based approach)[59] we estimate the costs for the maintenance of this tool to be as detailed in Table F.16 below.

Table F.16 Operating expenditure for a standards based online reporting application

Role	Description	Days p.a.	Posts required	Cost (EU official) (€)	Cost (private sector) (€)	Cost (NGO) (€)
Project Manager	Manages maintenance and updates	22	1	13,500	19,300	12,700
Application Developer	Designs application updates	22	1	13,500	16,000	10,700
Quality assurance & test	Tests the application updates	22	1	13,500	16,000	10,500
Total				**40,000**	**51,000**	**34,000**

Survey of systems characteristics, 1 February 2008 available at http://www.cen.eu/cen/Sectors/Sectors/ISSS/Activity/Pages/Tissues_and_cells.aspx (visited 12 February 2012)

[59] The proposed proxy has a much lower traffic requirement in terms of database inserts, updates and deletions than what might be envisaged in the case of the ECC. However, since coping with traffic load is more driven by the ICT infrastructure (bandwidth, CPU speed) relative to the application, the proxy remains suitable (since in the case of the ECC the ICT infrastructure would be provided by Europol)

Appendix G: Cost estimate breakdown "pathfinder phase" Jan–Dec 2013

In Table G.1 we present a breakdown of one-off expenditure and ongoing costs for the "pathfinder phase" of the European Cybercrime Centre from January to December 2013.

Table G.1 Pathfinder phase cost breakdown

Item	Description	Cost (€)
ECC governance team		
One off expenditure		
ICT infrastructure	Acquisition of three Desktop ICT infrastructure suitable to be used in EHQ	12,000
Ongoing expenditure		
Two functionary staff	EU-level AD (Restricted) post	262,000
One admin assistant	EU-level AD (Restricted) post	131,000
Travel and subsistence	Cost of two personnel visiting EU27 + other countries	50,000
ICT support & maintenance	Included in EHQ operating costs	nil
Studies and research	Research exercises to develop procurement of forensic equipment; interactions with non-LEA stakeholders, etc.	120,000
Publications & communications	Printing and design costs for ECC publications; branding, etc.	50,000
First meeting of ECC Capability Board	Costs to cover two-day meeting of 20 persons on ECC Capability Board	83,000
Other	Other miscellaneous costs	5,000
Criminal intelligence analysis and operational support		
One off expenditure		
Provide criminal intelligence analysis and operational support to MS	n/a	nil

Ongoing expenditure		
Provide criminal intelligence analysis and operational support to MS	n/a	as current status quo
Broad-based training, education and good practice		
One off expenditure		
Refresh of training materials	Based on 10 days of external expert time to review and update course content	70,000
Ongoing expenditure		
Extend basic (CPD) training to broader members of the criminal justice community (doubling number of five-day courses offered)	Delivery of an additional nine five-day courses per year by EU-level post	55,000
Travel and subsistence contribution	50% co-funding for 40 personnel to attend five-day training courses (as per current Europol delivery of five-day component of ECTEG-designed course) delivered by CEPOL	58,1000
Events	Costs of running events (based on CEPOL 2011 budget for such information events and expert meetings)	36,000
Best and good practice development	Preparation and dissemination of best/good practice for LEA (based on CEPOL budget)	100,000
Co-operation and co-ordination		
Data Fusion Unit		
One off expenditure		
ICT infrastructure	Acquisition of one Desktop ICT infrastructure suitable to be used in EHQ	4,000
Ongoing expenditure		
Data Fusion Analyst	One EU-level AD (Restricted) post	131,000
LEA–CERT PPP Network	75% contribution from ECC budget to MS level LEA–CERT Team	177,000
Data from private sector	Conclude contractual costs for data feed from private sector data providers	100,000
Travel and subsistence	Costs of DFU Analyst visiting three MS	15,000
ICT provision	Included in EHQ operating costs	nil
Guidance development	Costs of developing operating guidance (researching, analysing and understanding expectations of CERTs and LEA across the EU27) for national level CERT Liaison Officers and producing appropriate reference and communication material	100,000
European Cybercrime Resource Facility		
One Off costs European Cybercrime Resource Facility		

ICT infrastructure	Acquisition of three Desktop ICT infrastructure suitable to be used in EHQ	12,000
Operating expenditure European Cybercrime Resource Facility		
Two functionary posts	Head and Manager of ECN	262,000
One administrative assistant	Administrative support	131,000
Travel & subsistence	Costs of travel to various judiciary authorities for fact-finding (e.g. Germany; Finland)	15,000
ICT provision	In-built within EHQ	n/a
Interpretation	Costs of facilitation of interpretation between ECN and judicial authorities (based on CEPOL data)	55,750
Facilitating online victim/witness reporting		
One off expenditure		
Requirements gathering	Commissioned requirement-gathering exercise to understand metadata in reporting systems from LEA, CERTs, private sector (sum based on ICROS model and other similar proxies – e.g. EISAS).	200,000
Online standards-based reporting tool	Commission, design, develop and deploy standards based online reporting tool	270,000
Ongoing expenditure costs reporting platform		
Application maintenance	Application updates and support	52,000
Other ongoing expenditure		
Training and security accreditation	Costs for recruitment of new posts (e.g. from external sources) to be security cleared and vetted, induction with Europol systems and infrastructure and training on required products and software (e.g. EIS)	300,000
Total labour expenditure		**920,000**
Total one-off expenditure		**565,000**
Total ongoing expenditure (pathfinder phase)		**1.94 million**
Contingency and programme risk	5% of total programme costs to account for unforeseen programme risk and contingencies	**171,000**
Total pathfinder phase		**3.62 million**