This product is part of the RAND Corporation technical report series. Reports may include research findings on a specific topic that is limited in scope; present discussions of the methodology employed in research; provide literature reviews, survey instruments, modeling exercises, guidelines for practitioners and research professionals, and supporting documentation; or deliver preliminary findings. All RAND reports undergo rigorous peer review to ensure that they meet high standards for research quality and objectivity.

TECHNICAL
REPORT

Feasibility Study for a European Cybercrime Centre

Neil Robinson, Emma Disley, Dimitris Potoglou, Anaïs Reding, Deirdre May Culley, Maryse Penny, Maarten Botterman, Gwendolyn Carpenter, Colin Blackman, Jeremy Millard

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

RAND EUROPE

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.

European Commission
DG Home Affairs, Directorate A
Rue du Luxembourg 46
B-1049 Brussels
HOME-PROCUREMENT-A4@ec.europa.eu

Published 2012 by the RAND Corporation
1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
4570 Fifth Avenue, Suite 600, Pittsburgh, PA 15213-2665
Westbrook Centre, Milton Road, Cambridge CB4 1YG, United Kingdom
RAND URL: http://www.rand.org
RAND Europe URL: http://www.rand.org/randeurope
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002;
Fax: (310) 451-6915; Email: order@rand.org

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.