

**ROB WAINWRIGHT,
EUROPOL DIRECTOR**

The European Cybercrime Centre (EC3) opened in January 2013, with the stated intention of supporting EU Member States in pursuing their cybercrime investigations. One year later, EC3 has already made significant contributions to a variety of complex cybercrime cases, and has plans to develop its capabilities even further in the coming year.

The investigators and analysts who joined EC3 from within Europol gave it the necessary impetus from day one; their operational experience has already been put to good use in some of the most complex and technologically advanced investigations Europol has ever supported. Their ranks have been bolstered by an enthusiastic team of newcomers who are contributing the latest cyber know-how and helping EC3 to strengthen its partnerships with the global law enforcement and judicial communities, CERTs and the private sector.

In 2014, I expect EC3 to make use of its newly opened Multi-Disciplinary Centre for Cyber Innovation (MDC-CI) to support and coordinate an increasing number of cybercrime-related operations. 2014 should also see the publication of important new threat assessments to help police chiefs and policy-makers to tackle cyber-related crime phenomena.

EC3's progress in its first 12 months has been remarkable but, in such a rapidly evolving environment, we will have to remain agile in order to continue disrupting criminals' online activities and making cyberspace a safer environment.

**TROELS ØERTING,
HEAD OF EC3**

But all of this would not have been possible without huge support from our colleagues in other parts of Europol, the trust from our colleagues in the 28 EU Member States and the invaluable advice, tips and expertise from our stakeholders in the Programme Board.

Next year will be even more demanding. I very much hope that the European Commission, Council and European Parliament will continue to support EC3's development. Without this support we cannot assist our frontline colleagues in the Member States to protect our freedom and security on an Internet which we will all very soon be connected to - always, as will the criminals.

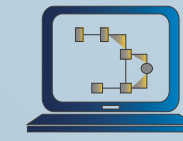
For me and for the staff in EC3, this first birthday is an occasion of great pride, satisfaction and joy. We opened our doors for business a year ago and since then have constantly developed and enhanced new services. Because we were relatively few in the beginning, each staff member needed to run faster, be more flexible and carefully prioritise a wider range of responsibilities than we originally planned. That was not always an easy task, but I am confident we managed. Now, at the end of our first year, I can conclude that we have more tasks, more operations and investigations than our present staff can cope with: that is actually a good sign of success.

OUTREACH

Creation of Advisory Groups to the EC3 Programme Board



Concrete steps for engagement of:
National law enforcement agencies
Private sector
Academia



CYBER INTELLIGENCE

Fostering information delivery by the private sector
Continuous scanning of open sources



More than 670 specialists are part of the SPACE community



The next generation of SPACE will include an Instant Messaging functionality with video and voice features, allowing real time communication between cybercrime experts.

TRAINING COURSES



6th forensic expert training on examination of skimming devices

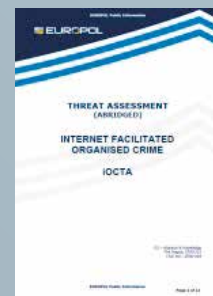


KNOWLEDGE PRODUCTS

STRATEGIC ANALYSIS



Strategic reports



iOCTA



Contribution to the SOCTA



Cyber Bits



Alerts & advice



EC3 Bulletin

DISCLAIMER

'2013: Our first year' is the exclusive property of Europol. Its content and layout, including -without any restriction- names, pictures, designs, texts and other graphical representations are protected under copyright and cannot be used or reproduced without Europol's prior written permission. The materials contained in this publication are provided by Europol staff members or private individuals working with Europol. To Europol's reasonable knowledge, all published material is original, legal, decent and truthful, complying with laws and regulations, does not infringe the Intellectual property rights of any third party, and is not defamatory, unreliable or misleading. However, Europol offers no guarantee of the accuracy, completeness or timeliness of the information published and accepts no responsibility or liability with regard to any material published in this publication. To Europol's reasonable knowledge, all photographs depicting private individuals and other visual materials used in this publication have received the consent of its subject and are used lawfully. The materials contained in this publication represent private opinions expressed by the authors and do not necessarily express those of Europol. Europol shall not be responsible or liable, directly or indirectly, for any damage or loss caused or alleged to be caused by or in connection with the use of or reliance on any such content of '2013: Our first year'.

CREDITS

Pictures: Arturas Gudavicius, Lars van Mulligen, Shutterstock
Design & edition: Iria Belenguer & Marco Feuerstein

**2013
OUR FIRST
YEAR**



2013 IN FIGURES

The European Cybercrime Centre (EC3), through its three Focal Points (FP) **Cyborg**, **Terminal** and **Twins**, is mandated to assist the Member States in combating the following forms of cybercrime:



Cybercrime committed by organised groups generating large criminal profits



Cybercrime causing serious harm to victims



Cybercrime affecting critical infrastructure and information systems in the EU



EC3 goes live

JANUARY



GLOBAL CREDIT CARD FRAUD NETWORKS DISMANTLED

44 arrested

15000

compromised credit card numbers retrieved

2 skimming factories dismantled



MARCH

EUROPEAN ACTION DAY TARGETS AIRLINE FRAUDSTERS



16 Member States

38 airports

More than **200** suspicious transactions reported by the industry

JUNE

Seizure of **€ 50000** and several thousand in e-currency



JUNE

13 arrests in total

RANSOM I & II

21000 compromised servers of companies located in **80** countries

DISMANTLING PROLIFIC POLICE RANSOMWARE CYBERCRIMINAL NETWORK

SEPTEMBER



EUROPOL - INTERPOL CYBERCRIME CONFERENCE 2013
24-25 SEPTEMBER 2013 THE HAGUE, THE NETHERLANDS



DECEMBER

ZEROACCESS BOTNET DISRUPTED

1.9M computers infected



COMBATING CHILD SEXUAL EXPLOITATION ONLINE



Identifying perpetrators and combating child sexual exploitation

Ongoing operations in several online environments supported: hidden services, P2P, websites, forums, web streaming and commercial distribution of child abuse material

IN TOTAL

440 CROSS-MATCH REPORTS

87 OPERATIONAL ANALYSIS REPORTS

57 JOINT OPERATIONS

30 KNOWLEDGE PRODUCTS

NEW CAPABILITIES

MDCCI Multi-Disciplinary Centre for Cyber Innovation



Digital Forensic IT Lab



LFE Large File Exchange system

EMAS European Malware Analysis System Secure and confidential dynamic malware analysis tool

