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 (MDCCI) 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 Oerting, Head of EC3

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.

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.

Outreach

Creation of Advisory Groups to the EC3 Programme Board

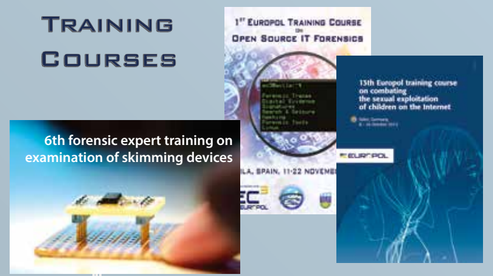
Concrete steps for engagement of:
National law enforcement agencies
Private sector
Academia

Cyber Intelligence

Fostering information delivery by the private sector

Continuous scanning of open sources

Training Courses



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.

Strategic Analysis

Knowledge Products

Strategic reports

iOCTA

Contribution to the SOCTA

Cyber Bits

Alerts & advice

EC3 Bulletin

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

2013
Our first year

EUROPEAN CYBERCRIME CENTRE
EC3
EUROPOL

EUROPOL PUBLIC INFORMATION

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 commited by organised groups generating large criminal profits

Cybercrime causing serious harm to victims

Cybercrime affecting critical infrastructure and information systems in the EU

JANUARY

EC3 goes live

MARCH

GLOBAL CREDIT CARD FRAUD NETWORKS DISMANTLED

44 arrested

2 skimming factories dismantled

15000 compromised credit card numbers retrieved

JUNE

RANSOM I & II

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

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

DISMANTLING PROLIFIC POLICE RANSOMWARE CYBERCRIMINAL NETWORK

13 arrests in total

JUNE

EUROPEAN ACTION DAY TARGETS AIRLINE FRAUDSTERS

16 Member States

38 airports

43 detentions

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

DECEMBER

ZEROACCESS BOTNET DISRUPTED

1.9M computers infected

COMBATING CHILD SEXUAL EXPLOITATION ONLINE

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

SEPTEMBER

EUROPOL - INTERPOL CYBERCRIME CONFERENCE 2013

24-25 SEPTEMBER 2013 — THE HAGUE, THE NETHERLANDS

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

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

LFE
Large File Exchange system