# CYBER INTELLIGENCE

Sharing knowledge, know-how and updates to enhance the fight against cybercrime

At Europol, generating cyber intelligence involves collecting information on cybercrime from a wide array of public, private and open sources, and then processing and analysing that information.

The objective is to enrich and expand the store of law-enforcement data and thus help make the fight against cybercrime as effective as possible. To this end, Europol has developed a number of cyber-intelligence products:

> Cyber Bits: short intelligence notifications on cyber-related topics
> the Open-Source Intelligence (OSINT) Dashboard, which aims to capture the most important events from the passing week in a broadly understood cyber domain
> the Common Taxonomy for the National Network of Computer Security Incident Response Teams (CSIRTs).
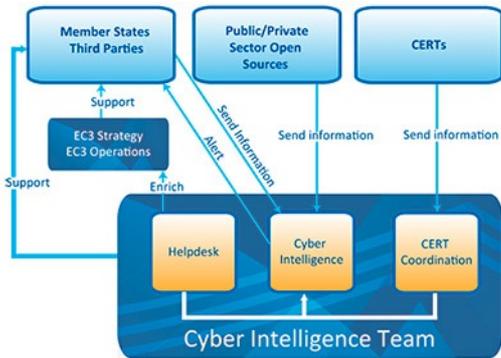
Cyber Bits

These notifications are designed to raise awareness and trigger discussions on further actions. Most are aimed at a broad audience, while a few are intended only for law enforcement authorities. Rather than providing a detailed assessment, they bring important news quickly to the attention of the law enforcement in Member States.

Notifications fall into four categories:

1. trends: updates on emerging patterns and on new modi operandi, tools and techniques that cyber criminals use

2. knowledge: guidance on different aspects of cybercrime such as infrastructure, tools and modus operandi

3. technology: news on technical developments that could have an impact on the work of law enforcement authorities, and that can spawn more in-depth reports if it is felt that the initial findings warrant this

4. tools: news on tools that have been developed at the request of a focal point within Europol, a Member State or a European Cybercrime Centre (EC3) stakeholder.
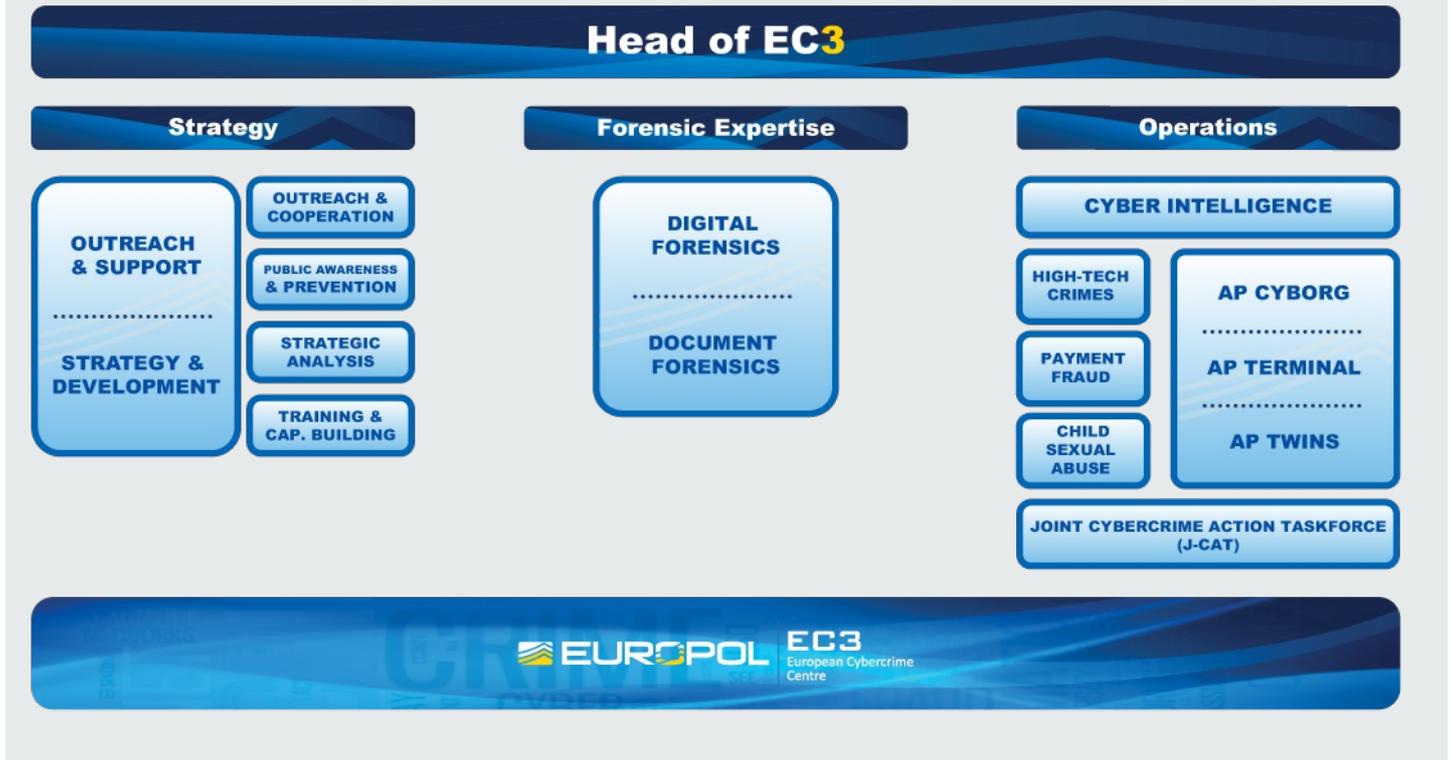
The OSINT dashboard

The OSINT dashboard is an accessible weekly update, highlighting for Europol's stakeholders the most important events in cyber security and cybercrime, with a focus on the work of EC3.

The Common Taxonomy for the National Network of CSIRTs

The Taxonomy sets out the common nomenclature for the classification of cyber incidents, attacks and events. It offers a technical perspective, but also includes a high-level legal categorisation to facilitate the harmonisation of incidents within the international network of CSIRTs, such as national law enforcement agencies, Europol and INTERPOL.

In order to improve cooperation both internationally and among all sectors involved in the fight against cybercrime, the Taxonomy links any cyber-event (such as a malware infection) to specific articles within two international legal instruments: the Convention on Cybercrime (ETS 185) and the Directive on Attacks against Information Systems (Directive 2013/40/EU). It thus fosters a unified approach to tackling cybercrime both immediately after an incident and during investigation and prosecution.

The document was developed within the framework of the EMPACT priority on cyber attacks and was prepared with the participation of the Portuguese judicial police and other Portuguese authorities. It takes its cue from the issuance by the European Union Agency for Network and Information Security (ENISA) of a Report on Information Sharing and Common Taxonomies between CSIRTs and Law Enforcement.

CRIME AREAS: Cybercrime
ENTITIES: European Cybercrime Center (EC3)
TARGET GROUPS: General Public • Law Enforcement • Academia • Professor • Students • Researcher • Press/Journalists