SERVICES & SUPPORT

A full range of crime-fighting tools and methods

Databases are just one component in Europol's service and support offerings.

This page gives an overview of the main elements of this support, with links to further pages where you can find out more.

International criminal and terrorist groups make use of the latest technology. Europol must therefore be equally flexible and innovative, and must ensure that it always has state-of-the-art tools and methods at its disposal, including databases and communication channels that offer fast and secure facilities for storing, searching, visualising, analysing and linking key information.

All Europol databases and services are available to staff and authorities in Member States 24 hours a day, seven days a week. We also send experts and make our services available via a mobile office, whenever requested by a Member State.

There follows a brief overview of each kind of service and support.

OPERATIONAL COORDINATION AND SUPPORT

Operational coordination is increasingly being recognised by EU Member States as a desirable and beneficial service, especially in large-scale operations involving several countries.

One of Europol's three main goals is to provide the most effective operational support and expertise to investigations in Member States by developing and employing a comprehensive portfolio of services.

Operational Centre

The Operational Centre, which runs 24/7, is the hub for the exchange of data among Europol, EU Member States and third parties on criminal activity.

More than 30 specialists and analysts work in this high-security unit.

All of Europol's operational and information and communications technology services are available to Member States. In addition, a mobile office can be deployed for on-the-spot support operations in Member States, thus providing a live connection to Europol's databases and platforms.

INFORMATION EXCHANGE

Secure Information Exchange Network Application (SIENA)

SIENA is a state-of-the-art platform that meets the communication needs of EU law enforcement.

The platform enables the swift and user-friendly exchange of operational and strategic crime-related information:

- among Europol's liaison officers, analysts and experts;
- among:
  - these analysts and experts;
  - Member States;
  - third parties with which Europol has cooperation agreements.

Europol Information System (EIS)

The EIS is Europol's central criminal information and intelligence database. It covers all of Europol's mandated crime areas, including terrorism.

Launched in 2005 and available in 22 languages , the EIS contains information on serious international crimes, suspected and convicted persons, criminal structures, and offences and the means used to commit them.

Europol Platform for Experts (EPE)

The EPE is a secure, collaborative web platform for specialists in a variety of law enforcement areas.

It facilitates the sharing of:

- best practices;

- documentation;
- innovation;
- knowledge;
- non-personal data on crime.

STRATEGIC ANALYSIS

Europol's strategic-analysis products help decision-makers identify priorities in the fight against organised crime and terrorism. Once that has been done, law enforcement officers can tailor their operational work nationally, regionally and locally.

INTELLIGENCE ANALYSIS

Europol is continually adapting the latest advances in technology to hone its advanced analytical capabilities. That way, its analysts can use the latest techniques and methods, among other things to identify links between international investigations.

Cyber intelligence

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 available law-enforcement data and thus help make the fight against cybercrime as effective as possible.

Cyber community engagement

Knowing more about the architecture and governance structure of the Internet will help the EC3 gain a better understanding of the internet governance landscape, and that in turn will help increase the effectiveness of cybercrime investigations by law enforcement inside and outside.

The EC3 runs an outreach function that develops and maintains partnerships to support the response of EU Member States to cybercrime.

Part of this work involves carrying out research into how the internet is governed, in order in turn to pinpoint significant vulnerabilities that organised crime groups can exploit.

In this context the EC3 works closely with:

- the Internet Corporation for Assigned Names and Numbers (ICANN)
- Réseaux IP Européens Network Coordination Centre (RIPE NCC)
- the Internet Engineering Task Force (IETF)
- other Internet stakeholders who play an important role in internet governance.

The aim is to increase the presence of law enforcement representation in this multi-stakeholder process. The Outreach and Support team in EC3 is working on a collective overview of law enforcement practices in the EU, in order among other things to affect policy on such matters as:

- IP address resolution
- criminal abuse of the domain-name system
- registration of accurate data
- the creation of a strong compliance mechanism for accredited registrars and registries.

FORENSICS

Forensics, or forensic science, involves applying the latest scientific methods to investigate and fight crimes in a range of areas. To this end, Europol provides forensic support to law enforcement agencies across the EU. The crimes Europol thus helps fight include:

- euro counterfeiting
- illicit drug production
- payment card fraud
- cybercrime.

TRAINING AND CAPACITY-BUILDING

The European Cybercrime Centre (EC3) supports the EU Member States law enforcement in capacity building and training, links available EU funding with law enforcement partners and centrally hosts high-tech services to support their national investigations.

The fast-paced development of cybercrime demands a quick and effective response from Europe's public services. Unfortunately, not all Member States possess an equal level of expertise in tackling cybercrime, thus are unable to combat the threat as effectively as others. The EC3 strives to address this imbalance by

ensuring equal access to the tools required to efficiently fight cybercrime. Moreover, the EC3 contributes to train law enforcement authorities in the latest methods of combating various cyber threats.

Public awareness and crime prevention

The EC3 plays a key role in preventing cybercrime in cooperation with EU Member State law enforcement agencies, in order to promote existing awareness-raising initiatives, and contribute to developing and delivering new ones, in cybercrime areas such as:

- online child sexual exploitation
- payment fraud
- other online threats.

Examples include:

- NoMoreRansom
- European Money Mule Action (EMMA)
- the Mobile Malware awareness campaign, part of the European Cyber Security Month (ECSM) 2016.

JOINT INVESTIGATION TEAMS (JITS)

A JIT is an investigative team that is set up for a fixed period and for a specific purpose, based on an agreement between or among two or more law enforcemen authorities in EU Member States. Competent authorities from countries outside the EU may participate in a JIT with the agreement of all other participating parties.

Read more about JITS

JOINT CYBERCRIME ACTION TASKFORCE (J-CAT)

Cybercrime knows no boundaries. Cybercriminals are constantly coming up with new ways to profit from their crimes at the expense of citizens, businesses and governments, across national borders and jurisdictions.

Police forces around the world thus encounter similar cybercrimes and similar criminal targets, and that calls for a coordinated, international approach to the problem.

The Joint Cybercrime Action Taskforce (J-CAT), which was launched in September 2014, fills that need. Located at Europol's European Cybercrime Centre (EC3) , it helps fight cybercrime within and outside the EU.

CRIME AREAS: Cybercrime • Child Sexual Exploitation • Forgery of money and means of payment • Payment Fraud
ENTITIES: European Cybercrime Center (EC3)
TARGET GROUPS: General Public • Law Enforcement • Academia • Professor • Students • Researcher • Press/Journalists

Source URL: https://www.europol.europa.eu/activities-services/services-support