Council of the European Union

Brussels, 23 May 2016
(OR. en)

8961/16

ENFOPOL 148

NOTE

From:	Europol
To:	Law Enforcement Working Party
Subject:	General Report on Europol's activities in 2015

1. Article 37(10)(c) of the Europol Decision[1] reads:

"*Each year the Management Board shall adopt:*

(…)

(c) a general report on Europol's activities during the previous year including the results achieved on the priorities set by the Council.

Those documents shall be submitted to the Council for endorsement. The Council shall forward them to the European Parliament for information."

2. The General Report on Europol's activities in 2015, adopted by the Management Board at its meeting on 11-12 May 2016, and submitted to the Council for endorsement by a letter dated 19 May 2016, is set out in the Annex.

3. On this basis, the LEWP is invited to take note of the report as set out in the Annex and submit it to COREPER and Council for endorsement.

[1] OJ L 121, 15.5.2009, p. 37.

The Hague, 19 May 2016

EDOC # 810623v4B

Europol Review 2015

General report on Europol activities

CONTENTS

FOREWORD

2015 was a challenging year for Europe and for its law enforcement community. The European Union was faced with an unprecedented influx of irregular migrants. More than one million migrants entered the European Union illegally in 2015. The vast majority of these journeys were facilitated by criminal networks, which have earned huge sums as a result.

In response to this situation, Europol reorganised its resources to assist the Member States and face the new security challenges effectively. Europol officers were deployed in hot spots in Italy and Greece, where the assistance was most needed, as part of the new EU Regional Task Force concept. In order to develop its services in this area further, Europol agreed to set up a European Migrant Smuggling Centre at its headquarters, which was launched in February 2016. This, however, has not been the only challenge.

The year's start and end were marked by terrorist attacks in Paris, which demonstrated the ambition and capability of the so-called Islamic State to inspire and execute highly organised international attacks. Europol did its utmost to assist the Member States in this difficult time. The Emergency Response Team at Europol supported France and Belgium 24/7 in their counter terrorist operations and providing analysis and delivering significant investigative leads. Europol's databases are now being systematically fed with critical information allowing for even faster and more effective identification of international terrorism links. Europol was also tasked by the Council of the European Union to upgrade its operational capabilities and create a European Counter Terrorism Centre at Europol, which was launched in January 2016. This was preceded by the creation in July 2015 of the EU Internet Referral Unit, responding to the spread of terrorist and violent extremist propaganda online.

For Europol these developments meant a dramatic increase in workload, a shift in operational priorities, and an increasing need to work 24/7 to analyse life-saving intelligence and provide crucial investigative leads in real time. This extra effort will continue in 2016.

Against this background, Europol continued to fulfil its mission and provide its services in other areas, in particular supporting Member States' concerted efforts to tackle the main serious organised crime threats. In the meantime, Europol has adopted a new Strategy for 2016-2020 which will provide strategic guidelines for the years to come. The legislative process for the adoption of a Europol Regulation also continued, bringing political agreement on the text in December 2015.

The Europol Review – General report on Europol activities[2] will inform you in more detail about the most important work that Europol has been involved in.

I am sure that cooperation with Member States and third parties will continue to bring tangible results: investigative links identified, attacks thwarted and organised crime groups dismantled. Europol has been preparing its capabilities and personnel to take on this challenge and fulfil its mission in the best possible way.

EUROPOL NEWS

Increasing cooperation to counter organised crime and terrorism

In 2015, Europol made significant progress as regards cooperation with the Member States and its partners: EU bodies, third states, as well as other international organisations. Cooperation with third parties with an operational cooperation agreement was especially strengthened through new associations with Europol's analysis work files. This trend reflects the ever increasing spread of organised crime and terrorism, and the matching need for law enforcement cooperation, also seen in the 20% increase over 2014 in the number of SIENA operational messages exchanged and over 60% increase in the use of the Europol Information System. Certain crime areas, such as illegal immigration and terrorism saw an impressive increase in operational cooperation and information sharing. The information regarding all persons registered in the analytical project on foreign terrorist fighters saw a six-fold increase from the end of 2014 till the beginning of 2016, and currently contains 18 000 persons (suspects or associates).

[2] The presentation of the *Europol review – General report on Europol activities* is done in accordance with Article 37(10)c of the Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office. The report is submitted to the Council of the European Union for endorsement and the Council forwards it to the European Parliament for information.

Interagency cooperation

Further to a joint annual report from Europol and Eurojust, the two agencies held a high-level meeting in 2015 to discuss their future cooperation. Moreover, Eurojust seconded an expert to the European Cybercrime Centre at Europol. Regular high-level meetings were also organised with Interpol and the two agencies agreed on common operational priorities.

Europol continued its close cooperation with Interpol. Both organisations hold an annual cybercrime conference. This year's edition took place at Europol's headquarters and brought together over 350 representatives from law enforcement, the private sector, academia and international organisations from around the globe. The cooperation between both organisations has been strengthened by the deployment of the first Europol liaison officer to the Interpol Global Complex for Innovation.

Europol signed an operational cooperation agreement with Frontex, to help tackle migrant smuggling networks more effectively. Europol also signed a grant agreement with the Office for Harmonization in the Internal Market (OHIM), which will intensify efforts in protecting intellectual property rights. Europol discussed further cooperation with the European Maritime Safety Agency (EMSA) and eu-LISA[3], while regular communication was established with the EU Counter Terrorism Coordinator.

European police chiefs stand together against terrorism

In September 2015, more than 300 police chiefs, senior law enforcement officers and academic experts from 50 countries and a dozen international organisations and agencies gathered at Europol headquarters in The Hague for the annual European Police Chiefs Convention (EPCC). During the event, the heads of European law enforcement discussed topical terrorism and illegal immigration issues. Illegal immigration was also high on the agendas of bilateral and multilateral meetings of police chiefs. Terrorism talks included the phenomenon of foreign fighters, and fighting terrorist and extremist propaganda content on the internet. The US perspective on fighting internet-related crime was presented in a keynote speech by James Comey, Director of the US FBI.

---

3 European Agency for the Operational Management of Large-Scale IT Systems in the Area of Freedom, Security and Justice (eu-LISA).

Europol's new Strategy for 2016-2020

In May 2015, Europol launched a rigorous consultation process with its key stakeholders to elaborate a new five-year Strategy, which was approved in December 2015 by Europol's Management Board. The new Europol Strategy 2016-2020 re-affirms Europol's core purpose and focus on supporting law enforcement authorities in their fight against serious and organised crime and terrorism. In this new stage of Europol's development, the strategic emphasis of the organisation will shift from the development of new capabilities to the full-scale delivery of operational services and impact. For the years 2016-2020, Europol will also concentrate focus on making a significant contribution to criminal information management in the EU.

Europol Regulation

The legislative process for the adoption of a Europol Regulation continued in 2015. The Council of the European Union and the European Parliament reached political agreement on the Europol Regulation in December 2015. Europol looks forward to the new flexibility this will bring for combating organised crime and terrorism, while maintaining a strong data protection and oversight regime. Europol anticipates spending most of 2016 in preparation for the implementation of the new legal framework, prior to its expected date of application in mid-2017.

Europol facilitates public access to documents

Europol has dedicated part of its website to providing public access to Europol documents. Additionally, a public register of documents is available and regularly updated. Europol also responds to requests for access to documents received both directly and through consultation by third parties. In 2015, Europol replied to 25 applications, 14 consultations and two confirmatory applications, corresponding to more than 100 documents.

EU Most Wanted

In 2015, Europol continued to support the European Network of Fugitive Active Search Teams (ENFAST) in developing a secure platform for the Europe's Most Wanted Fugitives' website. ENFAST is a network of police officers from 28 EU Member States specialised in undertaking immediate action to locate and arrest fugitives. As a result of this project, a dedicated website of WWW.EUMOSTWANTED.EU was launched in January 2016. The website available in 17 languages shares information on high-profile internationally-wanted criminals, convicted of, or suspected of having committed, serious crimes or terrorist acts in Europe. Within the first 36 hours after the launch the site was viewed by more than 1 million visitors. Three days after the launch, the first target on the list was arrested by the Helsinki Police.

Europol explores tomorrow's organised crime

Organised crime remains dynamic and continues to find ways of exploiting new and evolving technologies. Europol has identified a number of key driving factors for the evolution of serious and organised crime in the EU in the coming years, such as new forms of payment, e.g. virtual currencies, which will change how criminal actors transfer and launder the illicit proceeds of crime. Innovation in transportation and logistics are expected to provide organised criminals with greater mobility and new ways to traffic illicit goods. The report outlines a number of plausible developments in the future and aims to encourage law enforcement authorities to consider and explore the potential evolution of serious and organised crime.

Did you know this about Europol?

Did you know that Europol is also engaged in fighting the trafficking of endangered species of flora and fauna, which is a form of environmental crime? Although this is not one of our priorities, Europol has dedicated staff working on these issues. Europol provides the permanent secretariat for the Environmental Crime Network (EnviCrimeNet), ensuring that practitioners from all over Europe can be linked together. In 2015, the EnviCrimeNet and Europol finalised a year-long intelligence project on environmental crime supported by the Dutch Police and Dutch Food, Consumer and Product Safety Authority, and comprising data from 50 jurisdictions. Underreporting of this type of crime has been identified as one of the main issues.

Europol basic facts 2015

Analysts[4] - 105

Specialists[5] - 258

Liaison officers – 190

Others[6] - 387

Overall staff[7] - 940

Women – 33%

Men – 67%

Overall 2015 budget - EUR 95 426 894[8]

EU bodies, third states and international organisations, partners of Europol

[World map: countries mentioned below, highlighted in different colours for each category]

- 28 EU Member States.
- Operational agreements: Albania, Australia, Canada, Colombia, Eurojust, former Yugoslav Republic of Macedonia, Frontex, Iceland, Interpol, Liechtenstein, Monaco, Montenegro, Norway, Serbia, Switzerland, United States.
- Strategic agreements: Bosnia and Herzegovina, CEPOL, ECB, ECDC, EMCDDA, ENISA, Moldova, OHIM, OLAF, Russia, Turkey, UNODC, Ukraine, World Customs Organisation.

4 The category 'analysts' includes assistant analysts, analysts, senior analysts, strategic analysts and senior strategic analysts.
5 The category 'specialists' includes specialists, senior specialists and specialist translators.
6 The category 'others' includes project managers, research officers, technical officers etc.
7 The category 'overall staff' includes the before mentioned 'Analysts', 'Specialists', 'Liaison Officers and Others'.
8 Including the OHIM funding for the fight against Intellectual Property Rights infringements.

PEOPLE IN DANGER

Unprecedented influx of irregular migrants into Europe

The year 2015 saw an unprecedented increase in the number of irregular migrants and refugees attempting to enter Europe. This has led to an unseen scale of criminal activities recorded by Europol. The large and well-established international criminal syndicates have engaged in migrant smuggling. Being already specialised and well-organised, they have resorted to the most modern means, including the use of social media to recruit migrants. Many other criminal networks are new to migrant smuggling – they go where the opportunity is high and risk low. It is assessed that one-third of these groups has been involved in other criminal activity: drugs, money laundering and trafficking in human beings, targeting for example unaccompanied minors among the irregular migrants who are especially vulnerable to further exploitation.

It is assessed that more than one million migrants entered the European Union illegally in 2015. Debriefings with the migrants at their points of entry suggest that 90% were brought into Europe by facilitators.

In view of this unprecedented crisis, and responding to the needs expressed by the European Union Member States, Europol restructured and reinforced its capabilities, specifically strengthening the role of its dedicated analysis project (focal point) and the Joint Operational Team (JOT) Mare dealing with the facilitation of illegal migration. The goal has been to improve the sharing and exchange of information aimed at targeting and disrupting people smuggling networks. Europol has also put a lot of resources to aid ongoing operational activities, including the deployment of its officers and databases in the so-called hot spots.

Joint Operational Team (JOT) Mare

JOT Mare was launched in March 2015 and is housed at Europol headquarters, with the involvement of seconded national experts from seven EU Member States. This joint operational team makes use of Europol’s unique intelligence capabilities, to exchange vital information in real time to disrupt networks operating from Turkey, Libya and other North African countries who are responsible for transporting migrants in life-threatening conditions.

ENRIQUE MORALES

Europol analyst since 1 December 2011

Born:	Madrid, Spain
Most recent locations:	Madrid, Spain, National Police
Education:	Degrees in Law and Political Science
Working experience:	9 years
Specialisation:	Analysis, illegal immigration, trafficking in human beings

Joint Operational Team Mare is a unique team combining Europol expertise with EU Member States' experts on migrant smuggling, with a particular focus on organised crime groups involved in smuggling migrants by vessels in the Mediterranean. "The cooperation between Europol analysts and the national experts seconded by Member States has been crucial for the success of the project," says Enrique Morales, one of the Europol analysts working for JOT Mare since its inception. "2015, when JOT Mare was launched, saw a steep increase in data being exchanged between Member States and provided to Europol. The whole team worked under extreme pressure to assist national authorities in the affected Member States in the best way possible". With a pro-active approach, JOT Mare has not only supported the EU Member States from its headquarters in The Hague, but has also deployed officers to the EU Regional Task Force in Piraeus, Greece and Catania, Italy. The support provided by JOT Mare will continue under the new European Migrant Smuggling Centre.

Europol data on illegal immigration
• **38 600 suspects (10 735 new suspects in 2015)**
• **140 000 new communications in 2015**
• **> 100 suspicious vessels listed**

EU Regional Task Force (EURTF) in Catania and Piraeus

The regional task force was set up in June 2015 as part of the hot spot approach recommended in the European Commission's Agenda on Migration. Europol officers at the EU Regional Task Force work under the umbrella of Europol with the main aim of supporting frontline EU Member States by fast-tracking information exchange on facilitated illegal immigration, and by providing forensic support if requested by the national authorities in Greece and Italy. The goal is to identify the criminal networks responsible for migrant smuggling and to ensure a comprehensive European law enforcement approach. On the spot, Europol works closely with local authorities and other partners such as Frontex and EUNAVFOR MED.

Key activities:

- Real-time intelligence collection (from all landing proceedings, interviews, etc.)
- Direct cross-checks against Europol databases
- Forensic support (examination of electronic devices, document scanning)
- Tailored analytical support: because of direct contact with local investigators, Europol can better assess their analytical needs and provide tailored analytical products.

LARA ALEGRIA RIBEIRO

Europol specialist since 1 February 2013

Born:	Cascais, Portugal
Most recent locations:	Lisbon, Portugal, Portuguese Immigration and Borders Service
Education:	Degree in Law, Post-graduate studies on Procedural Forensic Practices
Working experience:	12 years
Specialisation:	Investigating organised crime groups, illegal immigration, trafficking in human beings and related criminality

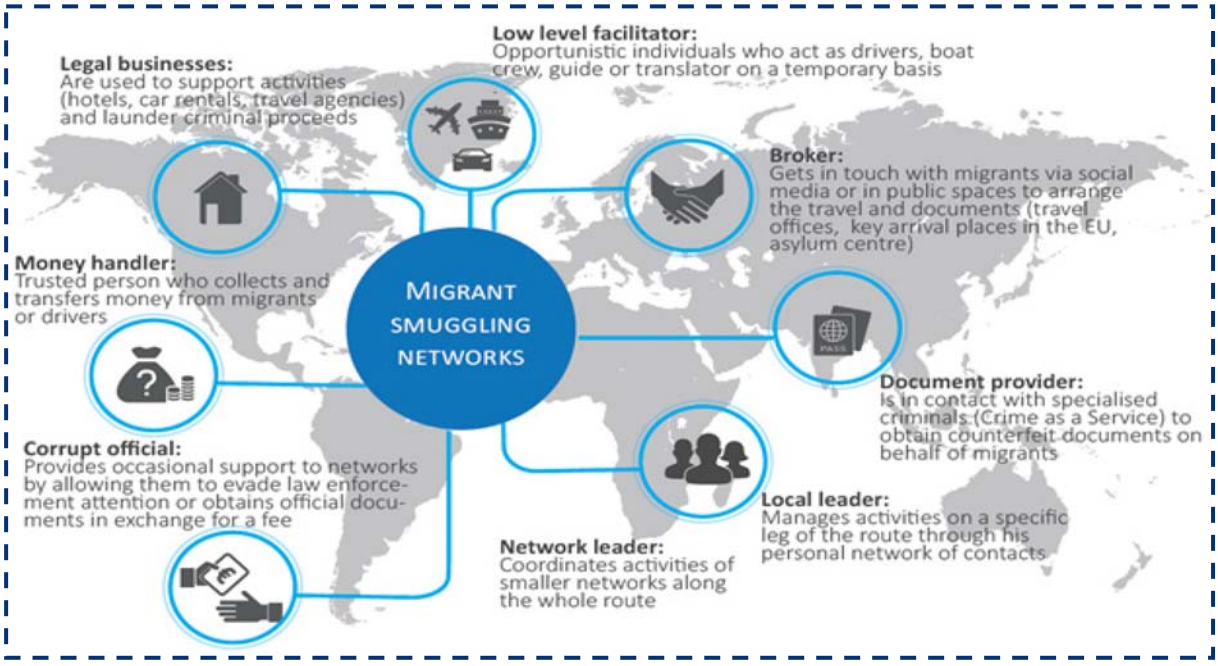
"Being present on the spot has brought an increased awareness to the national actors of the global and truly cross border phenomenon of organised criminality dealing with facilitating illegal immigration, and the need to pursue a holistic approach when tackling this type of criminality," says Lara. "The new role of Europol within the EURTFs and the hotspots, is clearly beneficial, not only to the countries of arrival which host the hot spots, but also to countries of transit and destination, with an overall benefit to the security of the European Union and the joint effort to fight organised crime".

European Migrant Smuggling Centre

Fighting migrant smuggling is a top priority for the European Union. The European Agenda on Migration tasked Europol with immediately strengthening its capabilities to result in a single entry point for inter-agency cooperation on migrant smuggling. The Justice and Home Affairs Council invited Europol to accelerate the establishment of the European Migrant Smuggling Centre (EMSC) to support Member States in better preventing and fighting migrant smuggling.

The EMSC will encompass the JOT Mare and will serve as an EU centre of expertise on migrant smuggling. The goal will be to support Member States in targeting and dismantling organised crime networks involved in migrant smuggling.

CRIMINAL SMUGGLING NETWORKS, 2015
Over 1 million migrants illegally entered the EU
More than 90% of migrants' journeys to the EU are facilitated by flexible and loose criminal networks, but also by individuals active along the routes and in key transit or destination hubs
People smuggling became a highly attractive and lucrative business **Criminal turnover: EUR 3-6 billion**
High-quality document counterfeiting is a growing illegal business for EU criminals



Source: Debriefings, 2015.

Criminal network organising deadly journeys of migrants disrupted

[Chart: operation presented in form of info-graphics]

October 2015, an international law enforcement operation against migrant smuggling and trafficking in human beings, coordinated by Europol

Participating states: 365 police officers from Spain and Poland, in both Spain and Poland.

Results:

- Arrests of 29 suspected migrant smugglers from an organised crime network responsible for facilitating deadly journeys for Pakistani migrants across the Mediterranean Sea (Libya-Italy and Turkey-Greece)
- 60 inspections of restaurants and 51 house searches in Poland and Spain.

Details: Investigators became aware of one of several routes and modus operandi used by the criminal network, and an incident (on 15 August) of a migrant dying while confined in inhumane conditions in a ship's hold. The identified ship and surviving migrants were consequently rescued by the Italian Navy. However, more than 40 people had died in the same hold when intoxicated by engine fumes. These victims had paid half the fee of those travelling on deck but were packed and transported in inhumane conditions.

The migrants paid around EUR 14 000 each to the criminal network for transport to Europe. In return, the facilitators offered them places in often unseaworthy boats, travelling across the Mediterranean. The criminal syndicate offered 'packages' to the migrants, which involved using forged documents to apply for residence permits, to register at the relevant city hall and to claim social security benefits. Residence permit applications were often linked to fake job offers, to work for kebab restaurants in Spain. Some of the profits earned by the criminal organisation were invested in opening new restaurants in different Spanish provinces, which were also used for the further labour exploitation of migrants. The remaining illegal profits were sent back to Pakistan through money wires, impersonating the identities of the exploited migrants without their consent.

Europol's Joint Operational Team (JOT) handled intelligence and provided criminal analysis and operational support during the common action days. Three Europol experts were deployed on the spot with the mobile office (two in Spain, one in Poland). Europol's analytical support resulted in the identification of links between this criminal group and previously-investigated organised criminal groups involved in the same criminal acts in Spain, using a similar modus operandi. Links made with other ongoing EU cases will be further explored.

EUR 10 million gain for an international gang dealing with migrant smuggling

[Chart: operation presented in form of info-graphics]

December 2015, a large-scale joint operation carried out by law enforcement and judicial authorities from Austria, Greece, Sweden and the United Kingdom, supported by Europol

Target: an organised crime group suspected of smuggling people into the European Union. The identified smugglers were mainly from Syria and Greece, but also Palestine and possibly Tunisia. The organised crime group is believed to have smuggled irregular migrants from Turkey (mainly individuals originating from Syria), then facilitating their journeys from Greece to other EU Member States via the Balkan route (former Yugoslav Republic of Macedonia, Serbia, Hungary, Austria, Germany and further northwards).

Results:

- 23 suspects arrested in Austria, Greece, Sweden and the United Kingdom.

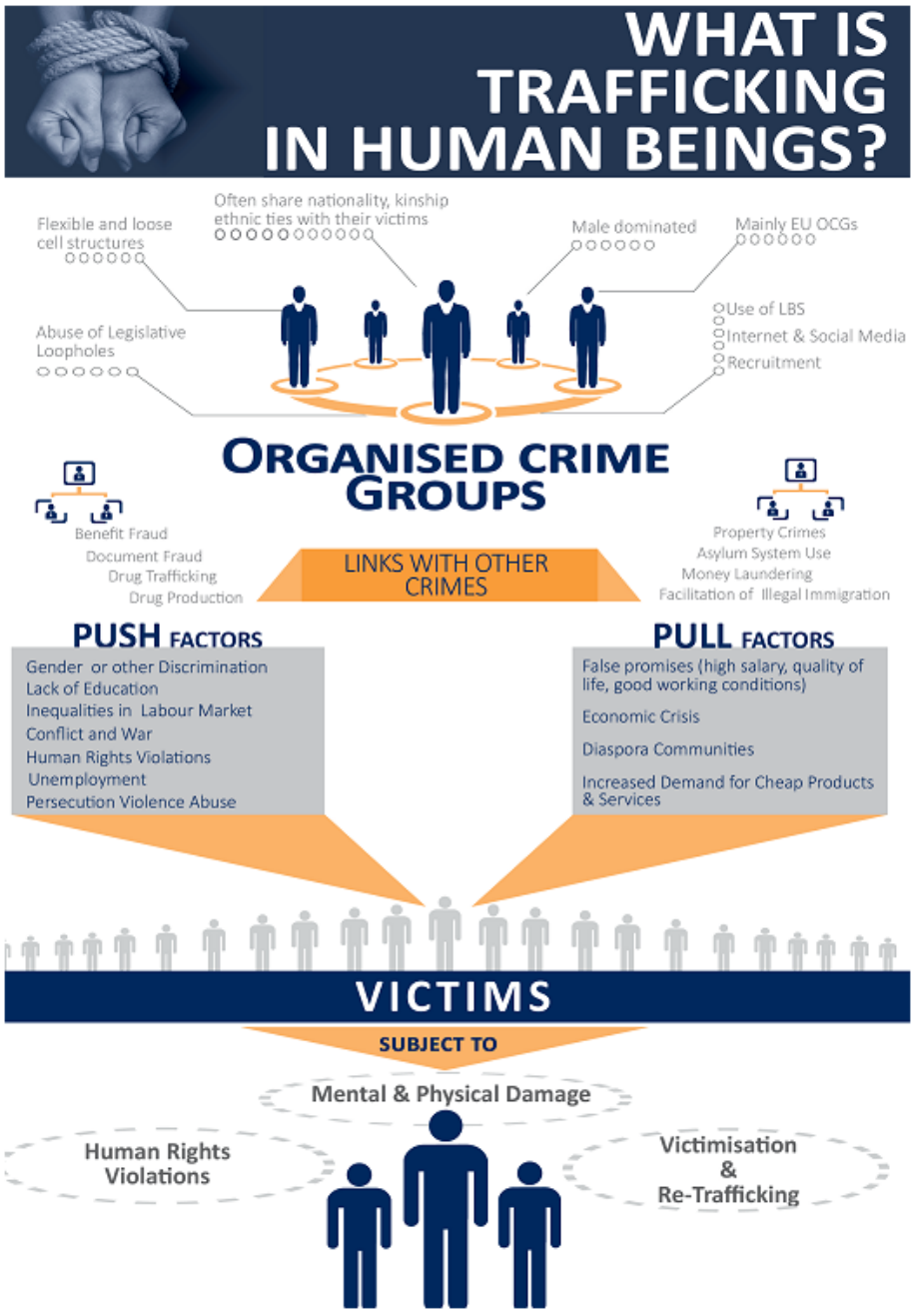
The members of the criminal network had set up their headquarters in Greece, where migrants – either located in Turkey or on their way to Greece – would contact them for further assistance with their journeys to Northern Europe. All forms of assistance could be provided ranging from transport and supplying forged travel documents, to housing. The migrants paid the facilitators via money-transfer services or simply with cash. This organised crime group is believed to have smuggled around 100 migrants per day and active since 2013. According to intelligence gathered so far, the total estimated earnings of the group were nearly EUR 10 million. During the action day, the organised crime group's leader was arrested by officers from the UK's National Crime Agency in Liverpool.

Europol supported the investigation from its early stages, by facilitating the exchange of intelligence between the involved Member States, performing cross-checks and real-time analysis of data, providing tailored analytical support to the investigators, and by financing and hosting operational meetings. Europol specialists and senior officers from participating law enforcement authorities coordinated actions from Europol headquarters in The Hague.

Trafficking in human beings

Once people have been smuggled into a territory, they become prone to other types of criminality and abuse. Trafficking in human beings (THB) occurs within national borders, and also within and outside the EU, and is often confused with people smuggling; however there are many differences between the two crime types:

- Consent: while the consent of a migrant to illegally enter a country is mandatory, in cases of THB the initial consent becomes legally irrelevant once the trafficker has used threats, coercion or fraud to exploit the victim
- Exploitation: in THB the person is further exploited after crossing borders
- Trans-nationality: THB takes place both across international borders (international trafficking) and within the borders of their own countries (internal trafficking), while facilitating illegal migration is only transnational
- Source of profits: in THB, profits are obtained from exploitation; in facilitating illegal migration, profits are gained from the transportation and facilitation of illegal entry or stay in another country.



'Lover boy' method employed to recruit sexual exploitation victims in Romania

[Chart: operation presented in form of info-graphics]

May 2015, a joint investigation by Romania and France focused on the criminal activities of an organised crime group active in Bordeaux.

Results:

- 56 houses searched
- 25 suspects arrested
- 11 victims identified
- EUR 5 million confiscated

The victims were recruited in Romania's Constanta region, using the 'lover boy' method[9]. They were trafficked for sexual exploitation to France, but also Germany, Italy and Spain. The group had well defined roles for its members, including those specialising in advertising the girls on French websites. The victims were forced into prostitution in different towns, and moved every few days to other locations. Based out of low cost hotels, the victims would be taken to clients' addresses by members of the group. Estimated profits of the criminal network: EUR 8 million, with EUR 5 million confiscated.

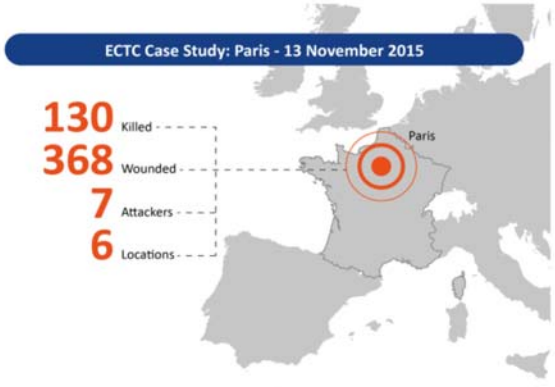
Europol supported the investigation on the action day in May by deploying an analyst with a mobile office in Romania to carry out cross checks and operational analysis on the spot. In earlier stages of the operation Europol cross-checked all requested criminal information against its databases, produced two cross-match reports and two operational analysis reports. To aid the operation's coordination, an operational meeting was organised at Europol headquarters.

[9] One of the methods that human traffickers use to attract vulnerable victims, typically by making contact and winning over the victim by promising a romantic relationship, with the aim of exploiting the victim through prostitution or unpaid labour.

TERRORISM

Islamic State going global

On the evening of 13 November 2015 three teams of terrorists, operating separately, committed a series of coordinated attacks with automatic rifles and explosives in a stadium, concert hall and at a number of restaurants and bars in Paris. The attacks were deliberately meant to kill and injure as many civilians as possible, and caused the death of 130 people, wounding 368. The so-called Islamic State (IS) claimed responsibility for the attacks, saying that they were committed in retaliation for the French airstrikes on IS targets in Syria and Iraq.



The attacks raised the question of whether IS is changing its prime focus from seizing territory and local resources to more global goals. Its involvement in international terrorism against the West was, until November, limited to attacks on tourists in Muslim-majority countries, and inspiring individuals in Europe to perpetrate lone-actor terrorist attacks. This apparent shift of focus of IS, and also the activities of other terrorist groups threatening the safety of the EU, is closely monitored by counter terrorism experts from EU Member States, supported by Europol specialists and analysts. The overall purpose of these efforts is to make timely interventions possible, and to react effectively to any terrorist activities.

New characteristics and modus operandi of the IS recent attacks
Mumbai style tactics
Development from series of lone-actor attacks to major terrorist attacks by an international network
Capacity to strike at will, at any time and at almost any chosen target, with a shift towards a broader strategy of IS going global
External action command trained for special forces-style attacks, in the international environment
Foreign terrorist fighters (FTFs) motivated less by religious zeal and more by social elements (role modelling, peer pressure, seeing themselves as military heroes not religious martyrs) **Significant proportion diagnosed with mental problems and with a criminal record**
The terrorist threat, like never before, is linked to other security phenomena such as mass migration, weapons trafficking, document counterfeiting and conflicts close to EU borders

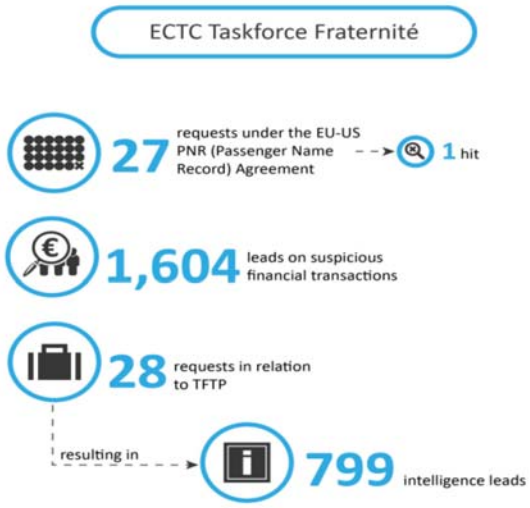
One issue, closely linked to IS and religiously inspired terrorism in general, and deserving special attention is that of returning foreign fighters. The November Paris attacks have once again demonstrated that young Europeans, having returned from Syria and other conflict areas where they had joined rebel groups, are of serious concern for the EU. Several of the Paris attackers, and people around them, had been to Syria before.

[Chart] Foreign Terrorist Fighters (FTFs) in Europol's dedicated analysis database

	December 2014	March 2015	June 2015	September 2015	December 2015	February 2016
Total persons	2850	4272	6609	10 479	17 623	18 197
FTFs	1022	1787	1925	1981	2167	4714

Chasing the terrorists and identifying missing links

Europol activated the Emergency Response Team (EMRT) immediately after the 13 November 2015 Paris attacks, to support the investigations on a 24/7 basis. Europol counter terrorism (CT) experts, analysts and French and Belgian colleagues worked round the clock to assist from Europol offices in The Hague and on the spot where investigations were taking place. They analysed an enormous amount of data generated by the criminal investigations being carried out in both countries. Altogether five mobile offices with staff members were deployed in Belgium, Paris and Lyon (Interpol) to assist French and Belgian investigators. This included expert Arabic language support from Europol's Internet Referral Unit.



Europol was able to demonstrate its ability to respond quickly and effectively to support counter-terrorism and criminal investigations whenever a major terrorist incident may require the investigations to have a transnational or international scope.

Adjusting our response to the new threat

Fighting terrorism, along with combating serious and organised crime, is Europol's core business. Europol's existing CT services have recently been brought together in the European Counter Terrorism Centre (ECTC), staffed by Europol experts and analysts, and operational from 1 January 2016. The ECTC maximises Europol's operational, technical and intelligence exchange capabilities.

These include monitoring Arab language terrorist websites and social media, and tracking terrorist support networks through information on financial transactions. The EU IRU - Internet Referral Unit – one of the core CT services composing the ECTC, identifies and analyses terrorist content on the internet and social media, and works with private sector companies to remove it.

The ECTC also houses the EU Bomb Data System (EBDS) a platform for the timely sharing of relevant information and intelligence on incidents involving explosives, incendiary and explosive devices, as well as chemical, biological, radiological and nuclear (CBRN) materials.

Fighting terrorist and extremist propaganda on the Internet

Terrorists' use of the Internet and social media has increased significantly in recent years. Via the Internet, terrorists can now reach millions of people through a single click. This gives them a powerful tool to reach their audiences. The number of Internet users worldwide is estimated at more than 3 billion people, according to the International Telecommunication Union (ITU)[10].

Jihadist groups in particular have demonstrated a sophisticated understanding of how social networks operate. They have launched well-organised concerted social media campaigns to recruit followers and to promote or glorify acts of terrorism or violent extremism. In doing this, they have been empowered by the use of Internet in unprecedented ways.

To tackle this phenomenon, on 12 March 2015, the Justice and Home Affairs Council of the European Union mandated Europol to establish a dedicated unit aimed at reducing the level and impact of terrorist and violent extremist propaganda on the Internet.

On 1 July 2015 Europol launched the European Union Internet Referral Unit (EU IRU) to combat terrorist propaganda and related violent extremist activities on the Internet. It would do this by:

- coordinating and sharing the identification (flagging) of terrorist and violent extremist online content with relevant partners;
- carrying out and supporting referrals quickly, efficiently and effectively, in close cooperation with industry;
- supporting competent authorities by providing strategic and operational analysis;
- being a European Centre for Excellence for the above-mentioned tasks.

[10] https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf.

In 2015, the EU IRU was still in its pilot phase and focused on targeting the main terrorist propaganda players. Europol experts followed the development of the jihadist propaganda, by highlighting major shifts in the jihadist narrative and interpreting the core messages broadcast by jihadist organisations. They produced early warning notifications on jihadist threats to EU Member States. From the EU IRU's inception in July, to December 2015, over 1700 decisions for referral were made. In more than 90% of cases, the content was deleted by the relevant online media platform.

Results from the EU IRU, July-December 2015

Referrals of terrorist and extremist propaganda:

- **1813 decisions for referral**
- **1605 removals**
- **89% total referral success rate**

Terrorist finance tracking

The size, structure and scope of terrorist organisations have evolved, and the methodologies to raise, transfer and use funds have subsequently adapted. Funds are required to carry out specific terrorist attacks: expenses may relate to travel to and from the target, the purchase of a range of arms and explosives or false identity documents, use of vehicles, mobile phones, covering of basic expenses, such as food, accommodation and medical treatment.

Europol's Terrorist Finance Tracking Programme (TFTP) has proven to be a valuable tool in terrorism related investigations. It enhances the ability to map out terrorist networks, often filling in missing links in an investigative chain. It is used to track terrorist money flows, allowing authorities to identify and locate operatives and their financiers, and assists in broader efforts to uncover terrorist cells. While the TFTP is based on queries linked to terrorism and terrorist financing, the generated leads enrich the overall intelligence picture, including the opportunity to identify new lines of inquiry (initially not related to counter terrorism).

Since January 2015 up to the end of January 2016, 50 contributions were submitted by the US authorities and 160 requests were sent by Member States and Europol, generating a total of over 9 400 intelligence leads, of relevance to 28 Member States. This includes close to 100 exchanges within TFTP concerning travelling fighters, leading to over 2 900 leads specific to this phenomenon. The TFTP also supported the investigations into the November 2015 terror attacks in Paris, generating more than 1000 leads so far.

Key trends and information on terrorism

Since 2007, Europol has provided law enforcement and intelligence officials, the European Parliament, Council of the EU, policymakers and the general public with facts and figures on terrorism in the European Union. Through its EU Terrorism Situation and Trend Report (TE-SAT), Europol also identifies developing trends in terrorism.

TE-SAT: reporting on the trends in terrorism and extremism in 2015[11]
205 terrorist attacks in the EU, of which the vast majority were attacks by ethno-nationalists and separatist groups
1053 counter terrorism-related arrests, of which the majority on suspicion of involvement in religiously inspired terrorism

[11] As reported by national competent authorities for the EU Terrorism Situation and Trend Report 2016.

CYBERCRIME

Cybercrime becomes more aggressive and confrontational

The European Cybercrime Centre (EC3) at Europol strengthens the law enforcement response to cybercrime in the European Union and helps protect European citizens, businesses and governments. Its focus is on cybercrimes:

- committed by organised crime groups, particularly those generating large criminal profits, such as online fraud;
- causing serious harm to victims, such as online child sexual exploitation;
- affecting critical infrastructure and information systems in the EU, including cyber-attacks.

The Internet Organised Crime Threat Assessment (IOCTA) is Europol's flagship annual strategic assessment of Internet-related organised crime. It informs decision makers on prioritisation of actions in the field of high-tech crimes, online child sexual exploitation and online payment fraud, and offers a forward looking, strategic overview of the cybercrime landscape. The 2015 IOCTA provides primarily a law enforcement perspective, combined with input from private industry, the financial sector and academia, which makes it unique compared to many private sector assessments.

The 2015 IOCTA reports how cybercrime is becoming more aggressive and confrontational. There is a shift from hidden, stealthy intrusions towards direct, confrontational contact between criminals and victims. This is seen across the various forms of cybercrime, including high-tech crimes, data breaches and sexual extortions. Aggressively confronting victims is the trademark of traditional organised crime groups who have turned to cybercrime for its high profits[12].

Cybercrime forensic expertise
The European Cybercrime Centre has an expert forensics team who provide network, mobile device and document forensics support. This expertise and analysis helps deliver evidence for ongoing investigations, while also providing Europol and EU law enforcement services with a better understanding of the tools and methods used by cybercriminals. In 2015, Europol provided on-the-spot digital forensic support to 20 investigations, including drugs and money laundering cases.

[12] IOCTA 2015(https://www.europol.europa.eu/iocta/2015/).

Data is a key target and commodity for cybercriminals

The number and frequency of publically disclosed data breaches is dramatically increasing. Such breaches, particularly when sensitive personal data is disclosed, inevitably lead to secondary offences as the data is used for fraud and extortion.

3.2 million computers infected with the Ramnit Malware

[Chart: operation presented in form of info-graphics]

On 24 February 2015, Europol coordinated a joint international operation to target the Ramnit botnet[13] that had infected 3.2 million computers around the world. This botnet was used by criminals to gain remote control of infected computers, primarily to steal passwords and disable antivirus protection. The malware, infecting users running Windows operating systems, exploited different infection methods such as links contained in spam emails. Representatives from the Member States' law enforcement services, Microsoft, Symantec and Anubis Networks worked together with Europol officials to shut down command and control servers and to redirect 300 Internet domain addresses used by the botnet's operators.

Participants:

- Lead: United Kingdom
- Law enforcement officers from: Germany, Italy, the Netherlands
- Partners from the private sector: Anubis Networks, Microsoft, Symantec
- Joint Cybercrime Action Taskforce (J-CAT), located at Europol
- Computer Emergency Response Team for the EU institutions, bodies and agencies (CERT-EU)

60 arrests in a complex cybercrime investigation

[Chart: operation presented in form of info-graphics]

[13] Botnet is a term used to describe a network of infected computers.

On 18 and 19 June, Europol's European Cybercrime Centre and Eurojust were involved in a coordinated action in Ukraine - joint investigation team (JIT) Mozart. JIT Mozart is one of the most complex cross-border cybercrime investigations that EC3 has to date supported, entailing more than 16 000 man-hours of investigative work, the exchange of more than 1700 operational messages, and intensive analysis of a large volume of complex data. EC3 supported the investigation by establishing the overall intelligence picture, and identifying crucial links between the malware attacks and the different investigations. Furthermore, Europol's analytical work and forensic analysis helped to link the suspects to the actual crimes and to identify the high-value top targets. Both Eurojust and Europol provided funding for the JIT. The substantial volume of data collected and processed during the investigation is still being used to trace the cybercriminals still at large, and has to date generated multiple hits with other high-profile cybercrime investigations.

Participants:

- JIT members: Austria, Belgium, Finland, Netherlands, Norway, United Kingdom
- Partner states: Estonia, Germany, Latvia, Moldova, Poland, Ukraine and The USA,
- Actions: one coordinated in Ukraine in June 2015; more operational actions in Austria, Belgium, Finland and the Netherlands
- Results: 60 arrests in multiple jurisdictions (Belgium, Estonia, Finland, Latvia, Netherlands, and Ukraine); dismantling of a sophisticated cybercriminal organised crime group responsible for attacking e-banking systems in Europe, America, Australia and Asia.

Cybercrime forum with up to 300 users taken down

[Chart: operation presented in form of info-graphics]

Darkode was one of the most prolific English-speaking cybercriminal forums in the world, used to trade and barter hacking expertise, malware and botnets, Zero Day Exploits, access to compromised servers, and to find partners for spam campaigns or malware attacks. The forum was a closed community of 250-300 active users. To join, potential candidates had to be invited and vetted by a trusted member of the forum.

Europol played a central coordination role in the takedown of Darkode, facilitating law enforcement activities prior to and during the actual operational action. Europol set up a dedicated command post with a direct secure communication link to the command centre in the US which was used to orchestrate the work effectively on the ground.

Participants:

- Lead: FBI, USA
- Law enforcement officers from: Australia, Brazil, Canada, Croatia, Colombia, Cyprus, Denmark, Finland, the Former Yugoslav Republic of Macedonia, Germany, India, Israel, Latvia, Nigeria, Bosnia and Herzegovina, Romania, Serbia, Sweden, United Kingdom, USA
- Joint Cybercrime Action Taskforce (J-CAT) located at Europol
- Takedowns and arrests coordinated from command posts set up by the FBI in Pittsburgh, USA, and Europol headquarters in The Hague, the Netherlands

Results: 28 individuals arrested, 37 houses searched, computers and other equipment seized.

Europol Malware Analysis Solution
The Europol Malware Analysis Solution (EMAS) is a dynamic, automated malware analysis solution provided by Europol to EU Member States. EMAS offers the possibility of creating analysis reports, but its most revolutionary feature is to produce intelligence for police investigators. Automated cross-checks can show links between attacks performed in different countries with the same malware, or with the same criminal organisation behind the same malware family, connecting to the same domains and related to different investigations within or outside the EU. In 2015, EMAS became fully automated to allow direct access to law enforcement parties with which Europol has operational agreements. In 2015: 525 108 files were analysed in EMAS, out of which 356 863 were identified as malicious.

Joint Cybercrime Action Taskforce (J-CAT)

The J-CAT is a country-led innovative framework for strengthening operational cooperation in fighting cybercrime, and operates from Europol's headquarters and is supported by Europol's European Cybercrime Centre. The J-CAT started as a six-month pilot in 2014 and was consequently extended. This extension came after the J-CAT successfully supported a number of important operations covering:

- high-tech crimes involving malware, botnets, and intrusion;
- crime facilitation (bulletproof hosting, counter-anti-virus services, infrastructure leasing and rental, money laundering, including virtual currencies);
- online fraud (online payment systems, carding, social engineering);
- various forms of online child sexual exploitation.

In 2015, the J-CAT was involved in eight successful operations, including operations Triangle, Bugbyte, Bluebonnet, R2D2 and B58 (Dorkbot), as well as one international crime prevention campaign: Blackfin. These activities were in cooperation with the private sector whose involvement is essential for tackling cross-border cyber threats.

The last J-CAT meeting for 2015 was attended by the US Attorney General, who highlighted the excellent level of cooperation between Europol and the US Department of Justice in tackling cybercrime, and announced the temporary deployment of a US prosecutor to The Hague to work closely with Europol's European Cybercrime Centre and the J-CAT.

Trojan horse for Android used to steal information and money

Operation R2D2, led by German law enforcement authorities and supported by several other countries, targeted mobile malware and malware buyers. The specific malware in question was the DroidJack Remote Administration Tool (RAT)/Android crimeware tool (SandroRAT). The Trojan horse program for Android devices opens a back door on compromised devices. It also steals information, and poses risks to money, privacy, data integrity and device access. The operation resulted in 20 house searches and 10 arrests in Europe, and 18 hearings in the USA.

Over a million computers infected with botnet

Operation B58 resulted in the disruption of the Dorkbot botnet. The Win32/Dorkbot botnet has infected over a million computers in 190 countries worldwide since it was discovered in 2011. Commonly spread via USB flash drives, instant messaging programmes and social networks, Dorkbot causes damage by opening a backdoor on the infected computer, allowing for remote access and potentially turning it into a botnet. Investigators are in the process of determining the number of victims around the world that have been impacted by this botnet.

Card-present fraud on the decrease in Europe

Following the implementation of EMV (Europay, MasterCard, and Visa) chip card ('Chip and PIN') technology in the EU, card-present fraud has significantly reduced in Europe. This is because cardholders' confidential data is more secure on a chip-embedded payment card than on a card with a magnetic strip.

…and on the increase overseas

However, card-present fraud has migrated to those countries where EMV technology is not yet fully implemented. The level of illegal transactions overseas has therefore sharply increased, as cards cloned in Europe are being used to withdraw money in non-EU countries.

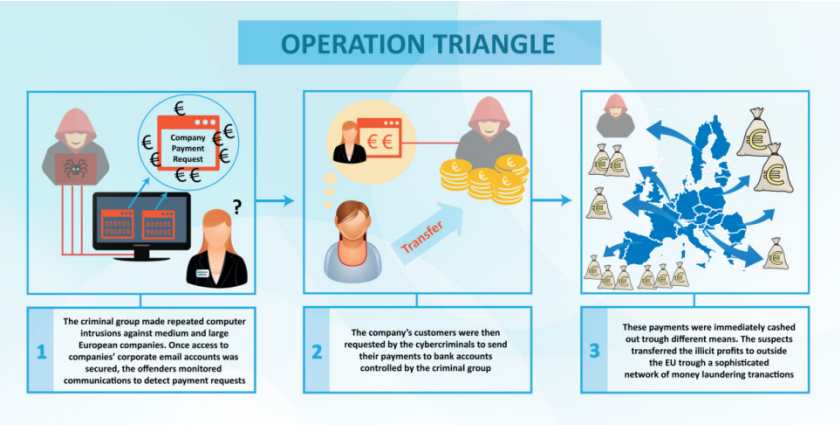
In March 2015, the Indonesian National Police (INP) contacted Europol regarding the arrest of several European citizens accused of card skimming in Bali. Since no cooperation agreement was in place with Indonesia, Europol contacted the national experts from the country of origin of the arrested criminals for any data relevant to the case. As a result of analysis performed within the Europol database, various cases of illegal money withdrawals were identified. All of them were made with payment cards issued by EU banks and skimmed in EU countries. It turned out that Indonesia was one of the most affected countries. Europol also identified the EU countries with the most recent withdrawals and ongoing cases. Subsequently Bulgaria, Denmark, Germany, Hungary, Romania, Slovenia, and Europol met with the Indonesian National Police, a local prosecutor, the Immigration Service and representatives from the seven biggest banks. Another meeting was organised to develop relations with key countries in the region.

Awareness meetings were organised in other parts of the world to raise awareness about payment card fraud overseas and money withdrawals in these regions, e.g. in Bogota, Colombia and in Singapore. The meeting in Colombia was of particular relevance, as it resulted in the launch of a joint cross-border investigation into an organised crime group operating both in Europe and South America.

Financial fraud cybercrime group dismantled

On 9 June 2015, the joint international operation Triangle led to the dismantling of a group of cybercriminals active in Belgium, Italy, Poland, Spain, the United Kingdom and Georgia. These cybercriminals were suspected of committing financial fraud involving email account intrusions. Operation Triangle resulted in the arrest of 49 suspects, 58 properties were searched, and numerous laptops and tablets, hard disks, telephones, SIM cards, memory sticks, forged documents, credit cards, cash, and bank account documents were seized. It was coordinated by Europol and Eurojust, led by the Italian Postal and Communications Police, the Spanish National Police, the Polish Police Central Bureau of Investigation, and supported by UK law enforcement bodies. The Joint Cybercrime Action Taskforce (J-CAT) at Europol also supported the operation.

[Chart]



More children exposed to sexual extortion

A growing number of children and teenagers own smartphones that they use to access social media and communication apps, and are increasingly present online. This facilitates the creation and distribution of large amounts of self-generated indecent material, making them vulnerable to sexual extortion. According to the UK media use survey, children aged 5-15 spend 12.5 hours online per week. 41% own a mobile phone, which increasingly have access to the internet, and 34% own tablet computers[14]. This trend will most probably increase exposing children even more to potential threats online.

Missing and exploited children

In 2015, Europol's European Cybercrime Centre extended information flow from the US National Centre for Missing and Exploited Children (NCMEC) to now include a total of 19 European countries: Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Greece, Hungary, Latvia, Luxembourg, Malta, Norway, Poland, Romania, Slovakia, Slovenia and Sweden. This improved set up was possible through cooperation with the US' Immigration and Customs Enforcement (ICE) who had a need to distribute NCMEC reports to EU Member States. US ICE provides Europol with information from the NCMEC tip line, which is then cross-checked by Europol and intelligence then provided to the concerned EU Member States. In 2015, more than **26 000** reports were disseminated.

Two-year-old girl rescued from sex abuse

A Romanian man suspected of sexually abusing his two-year-old daughter, filming the abuse and posting the child abuse material online, was arrested and the child rescued by Romanian law enforcement authorities.

[14] IOCTA 2015 (https://www.europol.europa.eu/iocta/2015/), p.33.

The case began when the US National Center for Missing and Exploited Children (NCMEC) received a report of suspected online child sexual abuse. NCMEC analysts passed the information to US liaison officers at Europol. Immigration and Customs Enforcement, Homeland Security Investigations (ICE HSI) special agents worked with the European Cybercrime Centre to immediately launch an investigation. Europol cross-checked and analysed all data, and produced an intelligence package for Romanian authorities. Romanian law enforcement authorities specialised in combating organised crime, and prosecutors, were rapidly involved. The suspected abuser, his victim and their location were soon identified. On 24 February 2015, Romanian police arrested the suspect and searched his home. Evidence found at the home matched that seen in the self-produced child abuse material that the perpetrator had posted online. The victim – the suspect's own daughter – was safeguarded.

Darknet used for exchanging child sex abuse material

Europol supported Italian law enforcement authorities to shut down a hidden service for distributing child sex abuse material online. The house of the Italian administrator was searched and 14 000 bitcoin wallets were seized.

Operation Babylon began two years ago, when the Italian Postal and Communications Police uncovered a hidden service within the Darknet that was facilitating the exchange of child sex abuse material. It was also servicing crime by hosting sellers of illegal commodities such as weapons, passport and identity documents, counterfeit and cloned credit cards, hacking services, and close to 210 sellers of drugs. The marketplace administrator earned a percentage from all of these transactions. The Italian State Police opened the investigation and was supported by Europol and undercover agents from the Italian National Centre for the Fight against Child Pornography Online (CNCPO). Investigators found thousands of online images of young victims being abused, which were being exchanged by paedophiles in many hidden online locations on the Darknet. Europol provided support and coordination during the operation, exchanged and shared vital information and intelligence, and deployed on-the-spot technical support in Campania, Italy.

Scanning the Internet for child abuse

The Virtual Global Taskforce (VGT) is a collaborative partnership of law enforcement agencies that have come together to combat online child sexual abuse worldwide. The 2015 child sexual exploitation environmental scan was commissioned by the VGT Board of Managers to set its strategic priorities for the next four years. It is a public version of an assessment for law enforcement drafted by Europol. Its main conclusions revealed how:

- the live streaming of child abuse is no longer an emerging trend, but an established reality
- the use of Tor in proliferating child sexual abuse material is a key threat
    - restricted areas pose the highest risk to children
- children are at risk of harm from online grooming and solicitation for sexual purposes
    - blackmail through the dissemination of sexually explicit material depicting victims.

Protecting children from sexual abuse

Europol is actively involved with the Lanzarote Committee of the Parties, which was established to monitor the implementation of the Convention on the Protection of Children against Sexual Abuse and facilitate the collection, analysis and exchange of related information and good practices. In 2015, highlights included the adoption of an opinion on online grooming and the creation of a first monitoring report on how children in Europe are legally protected against sexual abuse in the circle of trust.

Europol advocates crime prevention

Europol cooperates with law enforcement authorities and the private sector in crime prevention. In the area of cybercrime, Europol supported a number of events in November 2015 as part of Operation Blackfin, a cybercrime awareness raising campaign led by the UK National Crime Agency, and supported by Europol's European Cybercrime Centre and the J-CAT. Together with anti-virus companies, several pop-up events were organised across Europe and beyond (Colombia and Australia[15]). This initiative was aimed at educating the public about the threats they face online, and, most importantly, how to protect themselves. Law enforcement and industry partners offered advice to the general public at various locations, such as airports, shopping centres and train stations. In the UK alone, 2 500 people attended the campaign events. In Colombia, approximately 650 people attended the workshops and 85 infected PCs were discovered.

The Cybercrime Prevention Network was set up by Europol as an informal group that aims to join forces in communicating about cybercrime prevention and awareness. It is comprised of law enforcement prevention experts from EU Member States, with the participation of Interpol and the European Commission (DG Home). The network was consolidated in 2015 with an annual meeting taking place at Europol, and the development of a dedicated space on the Europol Platform for Experts (SPACE) for the exchange of best practices and expertise among its members.

Social media is increasingly becoming an inherent part of cybercrime prevention, with a large proportion of the target audience present online. Europol uses its Twitter account to provide updates on its latest activities, advice on prevention and awareness, and inform the public about other topics related to cybercrime and crime fighting.

[15] Australia aligned its national level cyber security awareness campaign with the Blackfin operation, but it was conducted in October prior to the actual week of action, and consisted of online rather than physical pop-up events.

Fighting the abuse of virtual currencies

In June 2015, Europol's Virtual Currencies Conference offered an exceptional line-up of speakers to explain the concepts behind virtual currencies, and present ways to follow the flow of transactions on blockchain[16] technologies and transactions to link criminals to crime. The event was organised for the second time by Europol and US ICE Homeland Security Investigations (HSI). The focus was on fighting the abuse of virtual currencies, such as Bitcoin, used for criminal transactions and money laundering. Participants were law enforcement practitioners involved in investigations of cybercrime, money laundering and asset recovery as well as representatives from the virtual currencies industry, the financial sector and academia. The conference launched a Tripartite Working Group between Europol, the Basel Institute and Interpol on the sharing of expertise concerning money laundering with virtual currencies.

News on the EU Financial Cybercrime Coalition

In June 2015, the second conference of the EU Financial Cybercrime Coalition was hosted at Europol with the aim of further strengthening cooperation between EU law enforcement and the financial sector. This annual conference is the largest event that brings together, at an EU level, law enforcement and the financial sector in the fight against cybercrime, and attracted 140 professionals from financial institutions and law enforcement services. The event resulted in several initiatives aimed at increasing the sharing of intelligence and further improving international law enforcement cooperation.

Training cybercrime experts

Europol's new course on Payment Card Fraud Forensics took place in July 2015 at the Spanish National Police Academy in Ávila, Spain. The aim of the training was to increase forensic experts' knowledge and expertise in the area of payment fraud forensics, such as the examination of skimming devices. During the course, 33 participants from various EU Member States learned about techniques to examine seized equipment, new trends and threats compromising card data and PINs in point-of-sale terminals and cash machines, as well as some payment card analysis tools. The course also covered ATM logical attacks, especially malware attacks, which are a developing threat in the area of payment card fraud. Europol also provides two other advanced cybercrime training courses: Combating Online Sexual Exploitation of Children and Open Source IT Forensics.

[16] A public ledger that contains all Bitcoin transactions ever made.

DRUGS

One third of EU organised crime groups involved in drugs trafficking

About one third of all organised crime groups in the EU are involved in the production and distribution of illicit drugs. Criminal networks exploit the demand for drugs in the EU and generate huge profits, often trafficking different types of drugs. The value of the European opiates market has been estimated at approximately EUR 12 billion. The most commonly used drug in the EU is cannabis followed by cocaine. Synthetic and narcotic drugs are big business and the EU is one of the largest and most valuable global markets for them.

Designer drugs on the rise

Organised criminal groups involved in the illicit production and trafficking of drugs are becoming increasingly sophisticated in their entrepreneurial outlook and many now market a range of new psychoactive substances (NPS), perhaps better known as ‘designer drugs’.

Over the past five years there has been an unprecedented increase in the number, type and availability of new psychoactive substances in Europe. More than 450 NPS have been reported since 2005, many of them posing a significant health threat to unsuspecting users who may consider them harmless, perhaps due to the fact they can be openly purchased either online or from retail shops. A number of serious adverse events have been seen in the EU, including deaths, where NPS drug users have experienced unexpected effects. Clever and aggressive marketing has created unprecedented demand for these products. The internet is well known for being a significant facilitator for serious and organised crime in general, however in the field of NPS it could rightly be described as a major driver of this phenomenon. This trend is expected to continue over the next few years.

Arguably the biggest challenge arising through the emergence of NPS is formulating a legislative framework that can respond rapidly and effectively to substances as they appear in the market. While market supply and demand grows in Europe for NPS, the absence of such legislation means that the manufacture and supply of these substances offers a low-risk/high-reward business arena for criminal groups to operate in.

NPS are defined as substances of abuse that are not under any international control. Main characteristics:

- **Not covered by drugs misuse laws**
- **Widely available - often in retail shops or via the internet**
- **Sold as 'not for human consumption'**
- **Brand names often similar to illegal drugs or intended effect**
- **Mimic effects of illegal drugs**
- **Most are manmade, although some occur naturally**
- **There is no 'safe' amount or way to take NPS.**

Europol addresses the issue of NPS robustly. It supports Member States to prevent and combat the illicit activities of criminal organisations relating to synthetic drug and NPS production and trafficking, as well as the diversion or supply of materials, equipment and precursors used to produce them.

Europol supports EU Member States in combating criminal networks engaged in synthetic drugs, NPS and precursors via:

- **Dedicated analysis file with analysts and specialised capabilities**
- **Expertise**
- **Facilitating investigations**
- **Dismantling drugs laboratories**
- **Training and publications (manuals, catalogues, bulletins)**
- **Early Warning System (EWS) which monitors new substances.**

More than 60 million cigarettes and 13 tonnes of drugs seized

Europol took part in a joint enforcement operation targeting NPS, which was organised by the World Customs Organisation (WCO) in collaboration with the Korean Customs Service. Many international organisations, including the International Narcotics Control Board (INCB), the United Nations Office on Drugs and Crime (UNODC), Interpol and Europol, participated in the initiative from an operational coordination unit at WCO headquarters in Brussels. The primary operational objectives were to identify, detect and seize smuggled consignments of NPS, investigate and dismantle distribution networks, and detect and close down websites selling and distributing NPS. As a result of 371 cases investigated, 13 408 kg of drugs were seized, including 1435 kg NPS-related. In addition, 61 million cigarettes, 1160 kg of items related to endangered species, firearms and bullets, EUR 315 000 and other taxable items were intercepted. This operation helped to expose new global trends in NPS abuse.

Operation Change targets European-Chinese organised crime network

[Chart: operation presented in form of info-graphics]

Operation Change was initiated by Europol in 2011. Intelligence from the EU Member States enabled the identification a Chinese national, who was a prolific manufacturer and supplier of illegal substances, and trying to keep one step ahead of legislation by making slight changes to the chemical compounds. The subject allegedly earned more USD 200 000 a day selling so-called designer drugs and it is strongly believed that a major organised crime network was involved in deliveries of controlled and non-controlled substances from China to both EU and international customers. The criminal network used legitimate companies to circumvent EU border controls. Analysis revealed that there had been at least 1000 shipments totalling 5.5 tonnes sent to 250 customers worldwide.

In cooperation with Eurojust, Europol initiated collaboration between law enforcement and judicial authorities in 17 countries. Europol facilitated the exchange of criminal intelligence, cross checking and analysis of data. More than 500 intelligence contributions were exchanged via SIENA, 21 analytical reports disseminated and 10 operational meetings organised. 40 suspects were detained in 11 EU countries and the US. Significant amounts of precursors and NPS were seized – more than 3.5 tonnes. The main target was arrested in China.

FRAUD

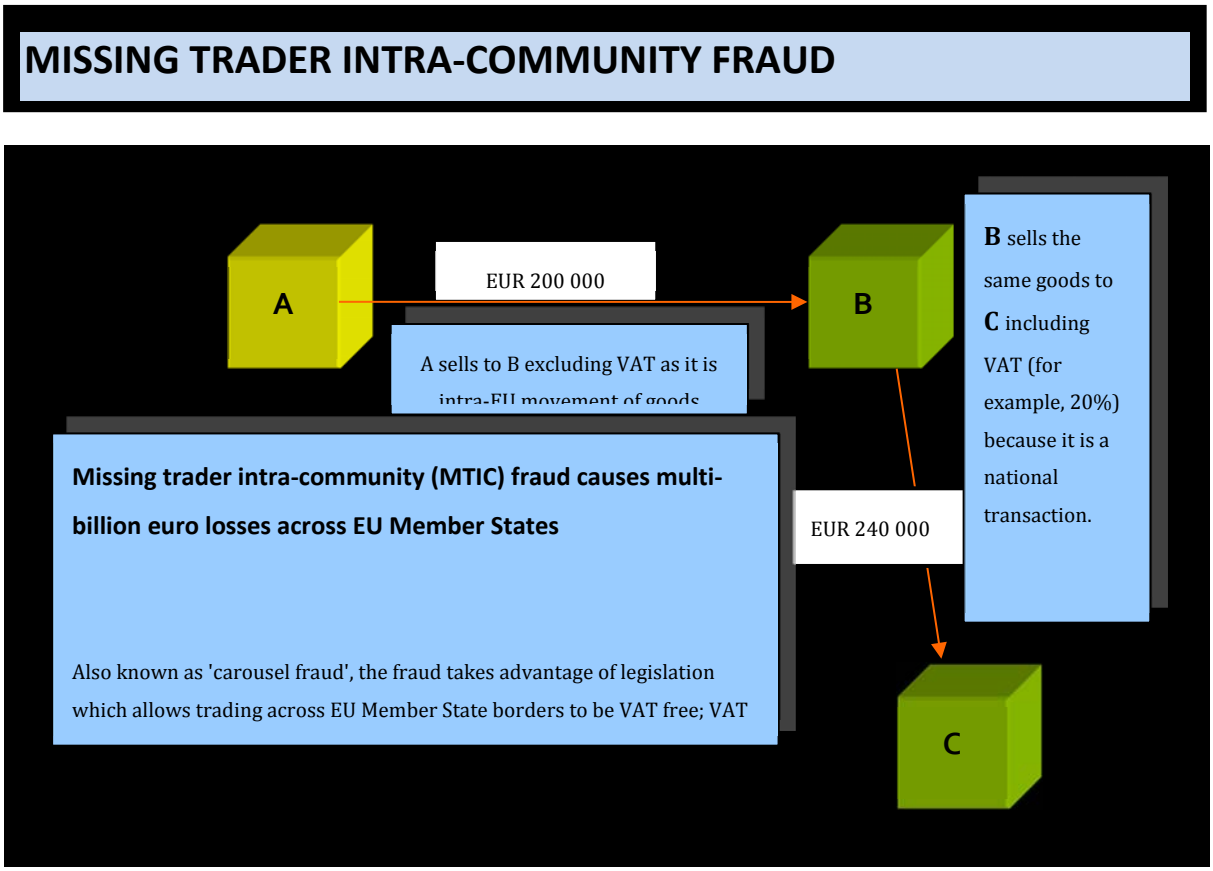
EUR 50 billion each year lost to VAT fraud

MTIC fraud is a form of organised, sophisticated tax fraud carried out by criminals who attack the value added tax (VAT) regimes of EU Member States. The activity is not a victimless white collar crime that only affects governments. By depriving EU Member States of tax revenues the criminals are effectively robbing EU citizens. Traditional missing trader intra-community (MTIC) fraud schemes involve goods such as precious metals, mobile phones or high-value portable electronic items. The more damaging organised crime gangs have mutated their activities into intangible markets, such as the environmental and energy sectors.

It is estimated that VAT revenue losses incurred by MTIC fraud alone are between EUR 45 billion and EUR 53 billion each year[17]. These profits are often used to fund other forms of criminality, such as cigarette smuggling or drugs trafficking.

The basic MTIC fraud model involves at least two Member States. The criminals create a structure of linked companies and individuals across these states who seek to exploit both national and international trading and revenue accounting procedures. Links between participants are disguised to make early detection more difficult. The initial entities responsible for the tax damage, the so-called missing traders, may only be in operation for a few months before disappearing.

[17] Based on the analysis of the VAT fraud gap in the VAT gap study commissioned by the European Commission, *Implementing the 'destination principle' to intra-EU B2B Supplies of Goods*, TAXUD/2013/DE/319, 30 June 2015, pp. 13-14.



Organised crime group behind EUR 320 million fraud scheme dismantled

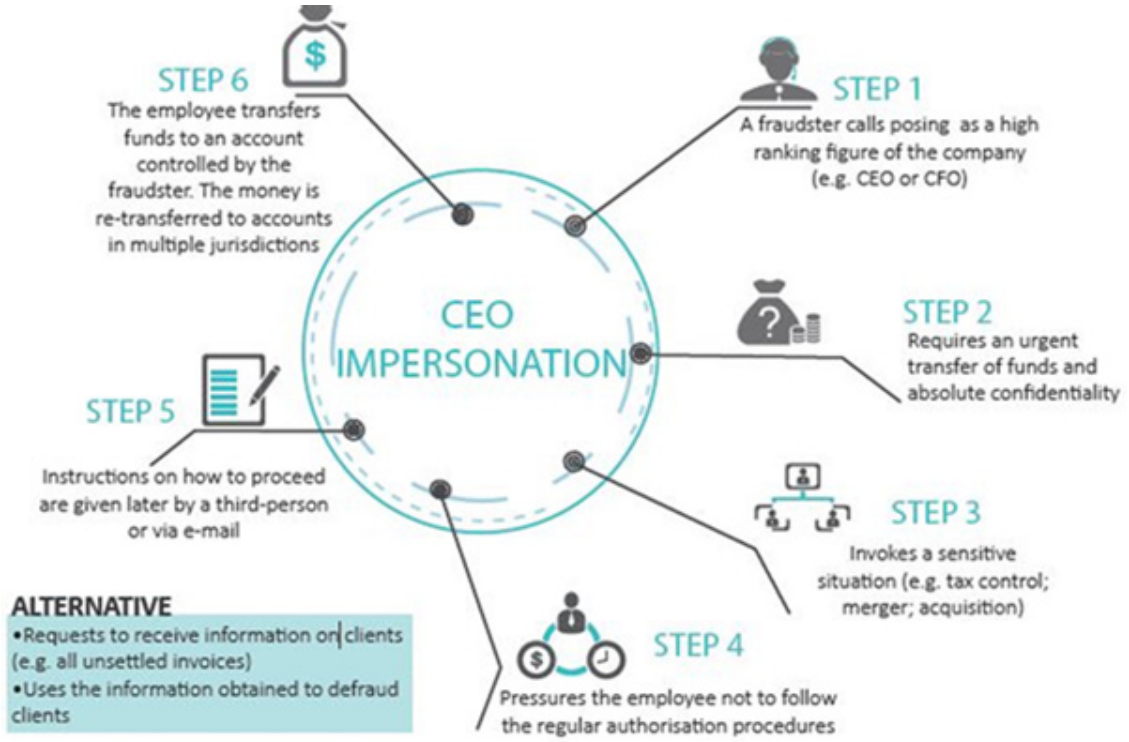
The joint investigation team (JIT) comprising four EU Member States - Czech Republic, Germany, the Netherlands and Poland - and supported by Europol and Eurojust, targeted an organised criminal group behind an MTIC fraud scheme in electronic goods worth EUR 320 million. The same JIT group targeted the organisers and facilitators of ‘alternative banking platforms’ across the globe, which were used to transfer crime-related proceeds and the associated money laundering of several hundred millions of euros. Results: 23 suspects arrested in nine countries; 27 witnesses heard; 117 premises simultaneously searched; assets and equipment seized in 15 EU Member States plus Ukraine and Gibraltar.

CEO fraud causes billion euro losses

Europol combats payment order fraud and, since October 2015, focuses more broadly on CEO fraud cases in Europe.

How does CEO fraud work? A fraudster calls a company employee pretending to be a high ranking figure of the company (e.g. CEO or CFO) who requires an urgent transfer of funds and absolute confidentiality. He mentions a sensitive situation such as tax control, merger or acquisition, and pressures the employee not to follow the regular authorisation procedures. The employee then receives information on how to proceed from a third person or via e-mail and transfers the funds to an account controlled by the fraudster. The money is re-transferred to accounts in multiple jurisdictions.

Illustration of the CEO fraud scheme



The FBI estimates the total loss to CEO fraud worldwide to be EUR 1.8 billion since 2010[18]. In Europe, it is estimated that in France alone more than 1500 companies lost about half a billion euros in that time[19]. Other EU Member States are also heavily affected by this type of criminality.

[18] Reported by the FBI at the International Mass Marketing Fraud Working Group in Brussels, November 2015.

EUR 11 billion lost to cigarette counterfeiting

Illegal tobacco factories provide organised crime groups with a huge source of income, which often goes towards funding other areas of serious organised crime and terrorism. http://www.kpmg.co.uk/email/06Jun14/OM014549A/PageTurner/index.htmlKPMG's Project Sun report assesses that in one year (data for 2014) the revenue lost by EU governments to counterfeit and contraband cigarettes equals to EUR 10.9 billion[20]. Excise fraud affects us all because the lost government revenue could have been spent on vital public services such as schools, hospitals, and law enforcement.

30 million cigarettes-worth of tobacco and cigarettes seized

[Chart: operation presented in form of info-graphics]

In February 2015, Europol supported the Hungarian National Tax and Customs Administration to dismantle a massive illegal cigarette factory near Budapest. The action was the result of intensive cooperation between various law enforcement agencies including customs, police and security services from five EU Member States, supported by Europol.

Participants:

- 5 Member States (Bulgaria, Czech Republic, Hungary, Netherlands, Slovakia)
- Europol

Results:

- 9 arrests of the Bulgarian organised crime group members who ran the factory
- 2.3 million cigarettes and 22 tonnes of tobacco – this amount would be enough to produce 30 million more cigarettes
- Complete, massive illegal cigarette factory dismantled.

---

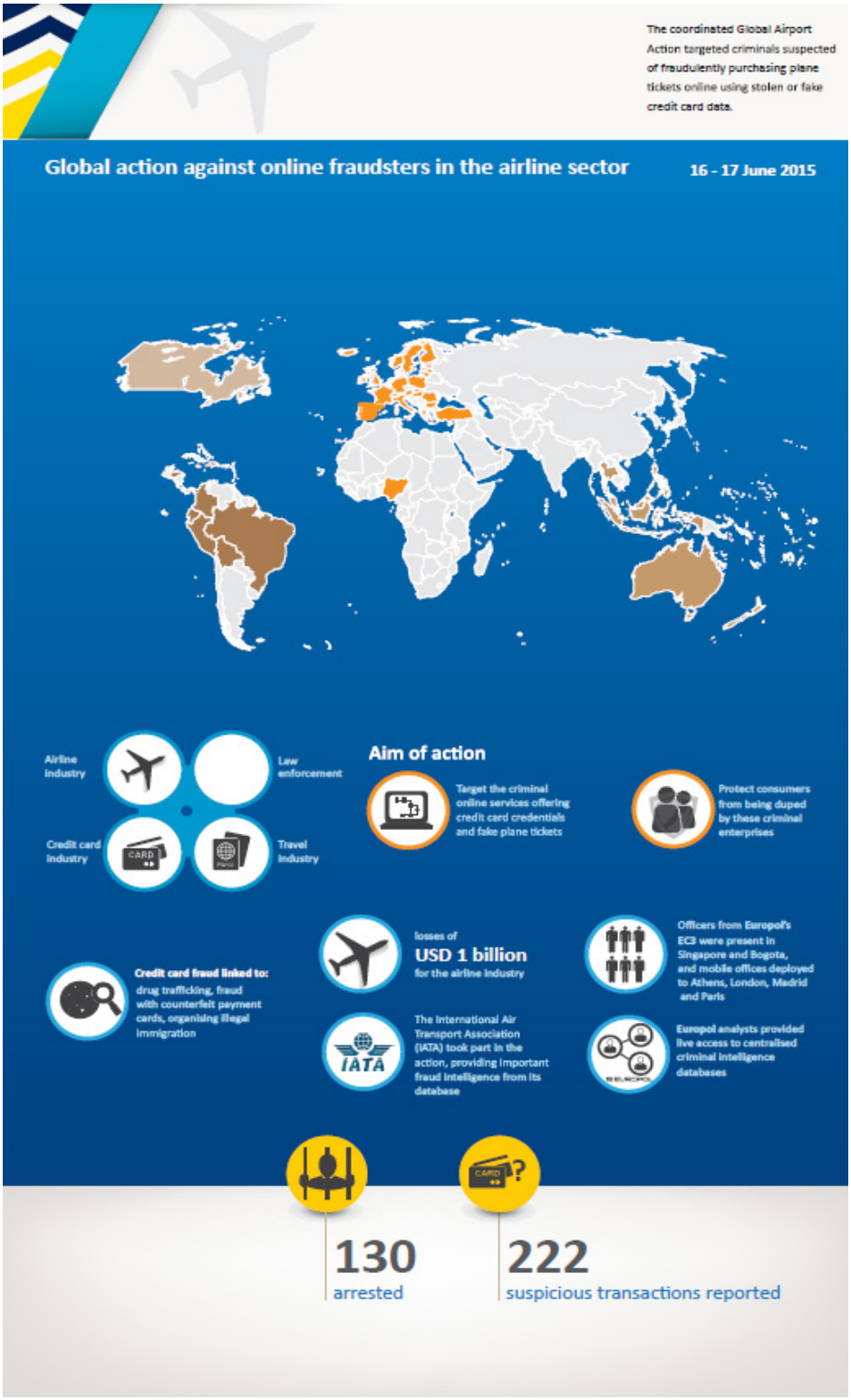
19 Reported to Europol by the French Office Central pour la Répression de la Grande Délinquance Financiére.

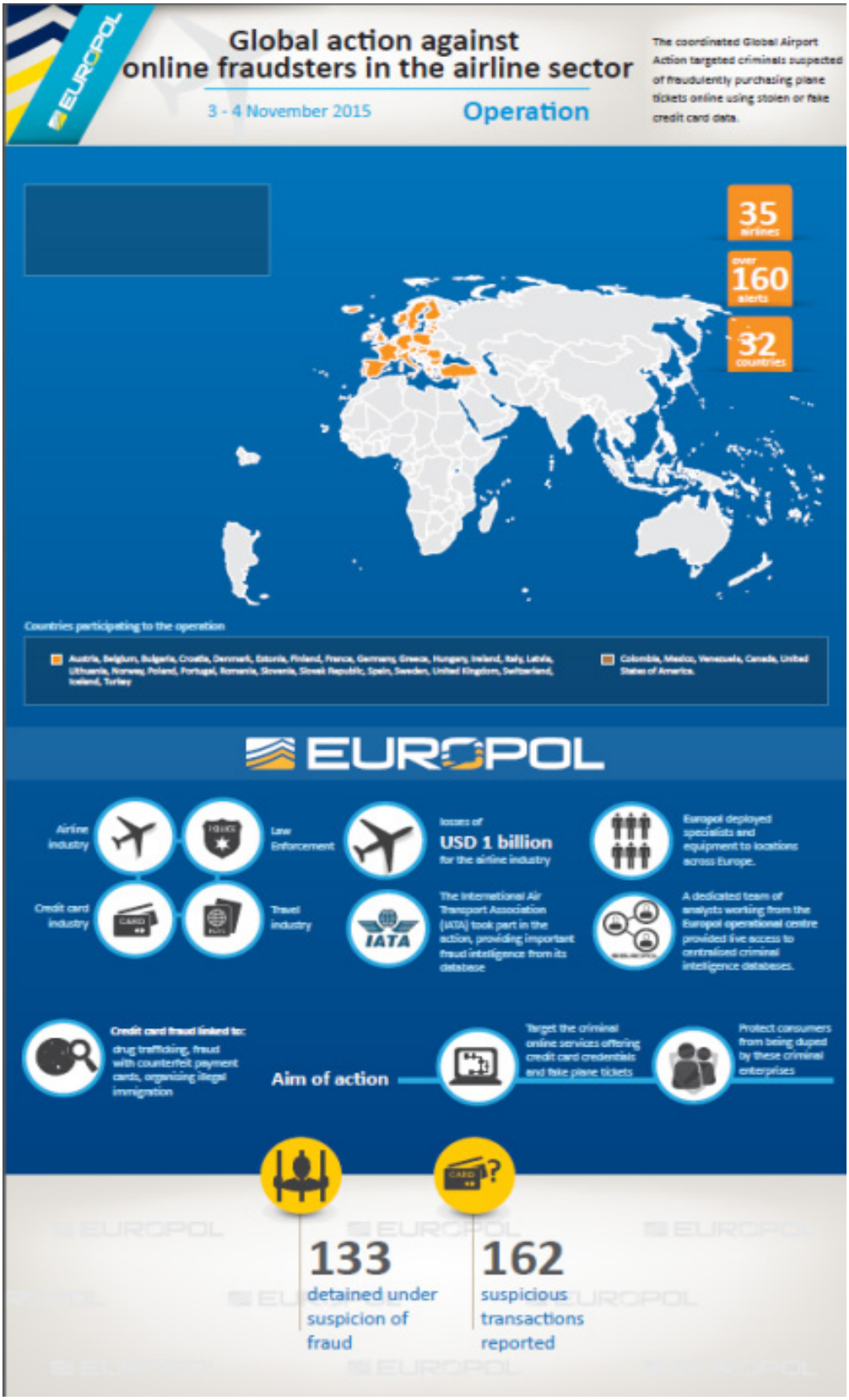
20 http://kpmg.co.uk/email/06Jun14/OM014549A/PageTurner/index.html.

The support Europol provided included intelligence sharing and development, crime analysis, and coordinated international collaboration and interventions. Europol also deployed a mobile office to the operational control unit in Budapest. This allowed information gathering during the raid, which was cross-matched against Europol's databases. Real-time feedback was then provided to officers on the ground during the operation.

Target: online fraudsters

Fraudulent online purchasing of flight tickets using compromised credit card data was the focus of the Global Airline Action Days on 16-17 June and 3-4 November, in which nearly all EU Members States participated as well as many third states. Europol coordinated the activities jointly with Interpol and Ameripol with assistance of Eurojust, Frontex and a large number of private sector partners. Additional support with mobile offices was provided by Europol in nine countries. The actions resulted in the arrest of 263 suspects originating mainly from North and Central Africa but also the Baltic States. The Global Airline Action Days triggered a number of investigations many of which revealed links to other crime areas, such as facilitating illegal immigration, cybercrime, trafficking in human beings and illicit drugs. Moreover, in some cases, fake online travel agencies were used to facilitate the credit card fraud.


The coordinated Global Airport Action targeted criminals suspected of fraudulently purchasing plane tickets online using stolen or fake credit card data.
Global action against online fraudsters in the airline sector
16 - 17 June 2015
Airline industry
Law enforcement
Credit card industry
Travel industry
Aim of action
Target the criminal online services offering credit card credentials and fake plane tickets
Protect consumers from being duped by these criminal enterprises
Credit card fraud linked to: drug trafficking, fraud with counterfeit payment cards, organising illegal immigration
losses of
USD 1 billion
for the airline industry
Officers from Europol's EC3 were present in Singapore and Bogota, and mobile offices deployed to Athens, London, Madrid and Paris
The International Air Transport Association (IATA) took part in the action, providing important fraud intelligence from its database
Europol analysts provided live access to centralised criminal intelligence databases
130
arrested
222
suspicious transactions reported



MONEY

Euro attractive to counterfeiters

The global acceptance of the euro as a stable currency with low rates of inflation makes it an attractive currency for counterfeiters.

The total amount of counterfeits found in circulation in 2015 stayed relatively stable compared to 2014. The EUR 20 banknote remains the most popular amongst counterfeiters, followed by the 50. Nevertheless, following a statement from the European Central Bank (ECB), euro banknotes continue to be a trusted and safe means of payment. The issuing of a new series of banknotes underlines this as the new design of the 20 euro gives new impetus to paper money. The enhanced security features, especially the window, makes this banknote one of the most sophisticated in the world.

Going global to fight euro counterfeiting

Europol works with partners within Europe and across the world to protect the euro from counterfeiting. Within Europe, Europol cooperates not only with police organisations but more and more with customs agencies too. Over the years Europol has established effective partnerships in South America, e.g. with Colombia. Many operations have also been coordinated with the United States Secret Service, which has expertise in fighting US dollar counterfeiting.

As the European Union’s central office for combating euro counterfeiting, one of Europol’s key functions is to act as the worldwide contact point for the subject. Europol is involved in all major euro counterfeiting investigations in the EU, including joint investigation teams, providing financial, forensic support and on-the-spot assistance.

Seizure of EUR 53 million worth of counterfeit banknotes

In February 2015, Italian authorities seized a large amount of counterfeit EUR 10, 20, 50 and 100 banknotes, with an approximate face value of EUR 53 million. The banknotes were hidden in the cellar of a building in Villaricca, Italy. This operation was supported by Europol. The specialised tracking equipment used by Italian authorities was financed by Europol. Financing investigative measures is one of the many ways Europol supports its partners in fighting euro counterfeiting.

Over 200 customers of counterfeit euros identified on the Darknet

Illegal trading platforms on the Darknet are increasingly being used by criminals to sell all kinds of illicit goods, including counterfeit euro banknotes. The forgery of money unit at Europol also focuses on this aspect of the phenomenon and provides intelligence to its partners. This resulted in a successful operation in the Netherlands that led to the arrest of one of the main dealers in counterfeit euro banknotes on the Darknet and the identification of over 200 of his customers. Subsequently, several operations targeting those customers were initiated by other countries.

Print shop of most detected counterfeit busted

In July 2015, a counterfeit euro print shop was dismantled in Frattaminore, Italy. This followed a long-running investigation that started in 2014 and focused on the production site of counterfeit EUR 20 euro banknotes. This denomination was, for many years, the most detected all over Europe. Europol assisted Italian law enforcement authorities with support on the spot, both technical and operational.

On site, over EUR 9 million in counterfeit banknotes was seized. This success seriously disrupted the production of counterfeits.

The money launderer in action

Things are seldom what they seem. Every day somewhere in Madrid a woman would go into a bank, accompanied by different people. Like a good Samaritan, she would act as an interpreter, assisting the people with opening bank accounts.

But, in fact, those people did not really want to open bank accounts, and she had no real desire to help them. She was in fact a controller and the people she 'assisted' were victims of trafficking in human beings (THB), forced to work in inhumane conditions in clothing factories run by a Chinese organised crime group (OCG). They were forced to open up bank accounts in their names to be used by the criminal group. This way, a vast network of accounts was created and, via smurfing techniques[21], large amounts of cash were placed and layered within the Spanish financial system.

When these activities raised some suspicions, the Spanish Financial Investigation Unit became involved. Preliminary checks were performed, the main group of 'smurfs' identified and it became clear that the total value of remittances was impossible to derive from labour-related activities. Spanish Guardia Civil was informed and a reverse financial investigation was immediately initiated to understand the origin of these substantial amounts of money. Soon enough, a large Chinese OCG based in Spain and operating in several EU countries was identified. It turned out to be a subsidiary of an even larger criminal network based in China. Europol was called in to assist.

The illicit profits were derived from importing counterfeit goods, excise tax fraud, exploiting Chinese workers in clothing factories on the outskirts of Madrid, and from the resulting sales of products without paying taxes due Several money laundering typologies were uncovered (smurfing, cash couriers and *fei ch'ien* - also known as the Chinese *hawala*). A total of EUR 300 million was estimated to have been laundered and sent to China.

[21] Using several agents, so-called "smurfs", to split a large financial transaction into several smaller ones. In this case different agents would perform deposits under the radar into the bank accounts controlled by an organised crime group. This is a typical modus operandi designed to avoid scrutiny by regulators or law enforcement agencies.

On 11 May 2015 this investigation, known as Operation Snake, concluded with a total of 32 suspects arrested, EUR 1 million in cash and 26 high-value vehicles seized, and 28 high-value real-estate assets frozen. This became one of the heaviest blows against Chinese organised crime activities in Europe. The Guardia Civil investigators followed the money trail further and found connections to other Chinese and Spanish criminal organisations. On 17 February 2016 Operation Shadow was launched, and resulted in the arrest of six top bank managers in Madrid. Europol supported this investigation by providing ongoing analytical support for over a year and by being present on the spot during operations Snake and Shadow.

Strengthening financial intelligence exchange

In 2015, work on the embedment of the FIU.net into Europol was finalised. FIU.net is a separate and dedicated information exchange network used by the European Union Financial Intelligence Units (FIUs). A decentralised network, FIU.net involves no central storage of information; when sending information from one FIU to another, the exchanged data is only, and securely, stored on the FIU.net databases at the premises of the FIUs involved in the exchange. The project to integrate the FIU.net with Europol capabilities was finalised in December 2015, allowing for the embedment of the FIU.net at Europol from 1 January 2016.

The embedding of the FIU.net into Europol was an important step in equipping Europol and the Member States with a broader and permanent type of interconnection, allowing for a structured and regular exchange of information. The FIU.net exchange platform has joined and strengthened other key Europol tools in the field, such as the Terrorist Finance Tracking Programme, dedicated analysis projects and EU Asset Recovery Offices' (AROs) cooperation coordinated by Europol.

EUR 2.4 billion from criminal activities frozen and seized annually in the EU

Organised crime activities are profit-driven, therefore confiscation is a strategic priority in the EU's fight against organised crime. The confiscation and recovery of proceeds from crime deprives criminals of what they have worked hard to acquire. Europol estimates that criminal proceeds to the value of approximately EUR 2.4 billion are frozen and seized annually in the EU. But before criminal proceeds can be confiscated by courts, they need to be traced and identified by law enforcement. Europol actively supports EU Member States to trace these criminal proceeds in Europe but increasingly also on a global level with the support of the Camden Asset Recovery Inter-Agency Network (CARIN) of asset recovery experts from 55 countries.

CONSUMER PROTECTION

Counterfeiting an increasingly profitable organised crime business

The 2015 Situation Report on Counterfeiting in the European Union concluded that the large-scale domestic production of counterfeit goods in the EU is becoming an increasingly profitable business for organised crime groups and organisations[22]. The report was written by Europol and the Office for Harmonization in the Internal Market (OHIM). It provides extensive information on the routes, entry points and modus operandi of the criminal networks actively producing and distributing counterfeit goods on EU territory. It also shows links between counterfeiting and other crime areas, using various case studies provided by EU Member States and private stakeholders.

Over 20 million counterfeit and potentially dangerous pharmaceuticals seized

[Chart: operation presented in form of info-graphics]

Europol works together with partners across the world to combat the distribution of counterfeit goods. In 2014, several successful operations highlighted the threat of counterfeit pharmaceuticals, food and drinks to consumers in the EU.

In 2015, Europol supported the largest ever, and eighth edition of, Operation Pangea which targeted counterfeit medicines and medical devices sold online. This global operation was coordinated by Interpol, from their coordination centre in Lyon. A record number of 115 countries, as well as international organisations and private sector companies, participated in last year's Operation Pangea.

Results worldwide:

- 429 investigations launched
- 20.7 million illicit and counterfeit medicines seized, worth an estimated USD 81 million
- 156 arrests
- 2414 websites selling fake medicines and products shut down
- 550 advertisements of illicit pharmaceuticals removed from the Internet.

[22] https://www.europol.europa.eu/content/2015-situation-report-counterfeiting-europan-union

Europol's contribution: cross-checking of all incoming data with Europol databases, producing analytical reports and identifying hits at the operational centre in Lyon (mobile office deployed), forensic support to Austria.

Operation Pangea has been successful in raising public awareness and fostering greater cooperation and communication between the participants. Its primary aim is to disrupt the activities of organised criminal networks operating online. This is achieved by shutting down websites, removing advertisements, disrupting payment services, intercepting illicit medicine in the postal system and supply chain, investigating the criminals involved in pharmaceutical crime, and raising awareness of the dangers associated with buying medicines online.

Operation Pangea is an annual cyclical operation which started in 2009. Results in the selected years:

	2010	2013	2015
Participating countries	44	99	**115**
Websites shut down	297	13 763	**2 414**
Seized packages	21 200	41 954	**50 000**
Arrests	87	213	**156**
Medicines (units) seized	2 300 000	10 192 274	**20 700 000**

Indonesia: Authorities uncovered an enterprise where criminals were altering the expiry dates or the amount of the active ingredients on packets of counterfeit, expired and unregistered medicines at a warehouse and returning them to a pharmacy for selling. Among the fake and illicit medicines seized during the operation were blood pressure medication, erectile dysfunction pills, cancer medication and nutritional supplements. In addition to interventions on the ground, the operation also targeted the main areas exploited by organised crime in the illegal online medicine trade: rogue domain name registrars, electronic payment systems and delivery services.

UK: Authorities discovered an illegal online pharmacy selling unlicensed medicines obtained from another country. Police and the Medicines and Healthcare Products Regulatory Agency raided a premises connected to the website and seized 60 000 units of potentially dangerous medicines worth an estimated USD 2.4 million.

USA: Investigations raised awareness of the growing health risk posed by the use of illicit or mislabelled silicone injections in cosmetic procedures. If they are used incorrectly, or contain substances other than medical-grade silicone, the injections can cause serious medical complications.

Google: Google's participation emphasised the importance of collaboration between law enforcement and the private sector in combating online pharmaceutical crime.

Europol helps target ivory and rhino horn smugglers

In 2015, Europol coordinated all operational activities within a series of global wildlife crime operations: COBRA III. Twenty-five EU Member States, Interpol and Eurojust participated in this operation under the umbrella of the EU Wildlife Enforcement Group. The operation targeted primarily smugglers of ivory and rhino horns who operate on the route from Africa via Europe towards the Asian markets (mainly Chinese and Vietnamese). The operation consisted of 70 complex investigations in 25 participating states and 600 seizures, including large amounts of new age medicine containing extracts from protected plants, and several thousand kilos of protected timber.

OPERATIONAL HUB

Law enforcement from 60 countries join forces to disrupt criminal infrastructure

In 2014, the large-scale 10-day Operation Archimedes was organised. In 2015, the concept changed into a series of Joint Action Days, which were more intelligence-led and regionally focused. Operation Blue Amber was this series of international actions to target organised crime, led by EU Member States and supported by Europol. The operation focused on EMPACT[23] priority crime areas such as drugs trafficking, irregular immigration, organised property crime and counterfeit goods.

Operation Blue Amber was a unique operation that led to law enforcement officers from 28 EU Member States, 32 non-EU countries and other international partners joining forces to disrupt organised crime groups and their criminal infrastructures. In 2015, several simultaneous interventions and action weeks took place across the world. Coordinated interventions took place throughout 2015 at airports, border-crossing points, ports and specific crime hot spots in towns and cities.

900 suspects arrested

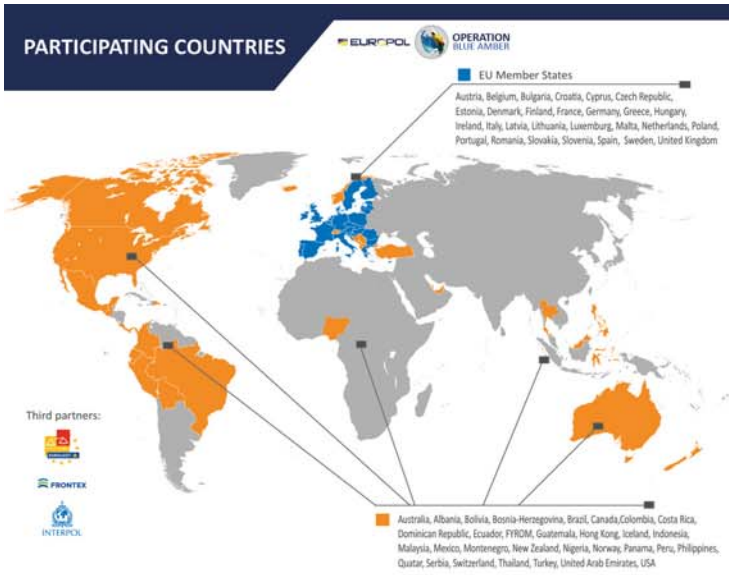
Nearly 900 arrests and 7.7 tonnes of drugs seized: these are only a few of the final results from Operation Blue Amber:

- Nearly 900 arrests made relating to drugs trafficking (257), property crime (281), and facilitation of irregular immigration (60);
- 263 arrests of fraudsters during the Global Airline Action days, which targeted criminals suspected of fraudulently purchasing plane tickets online using stolen or fake credit card data;
- 5 tonnes of cocaine, 2.1 tonnes of cannabis, 280 kg of synthetic drugs and 82 kg of heroin seized;
- 254 vehicles, 190 tonnes of counterfeit pesticides, and almost EUR 140 000 in cash confiscated;
- 1400 tonnes of stolen metal seized.

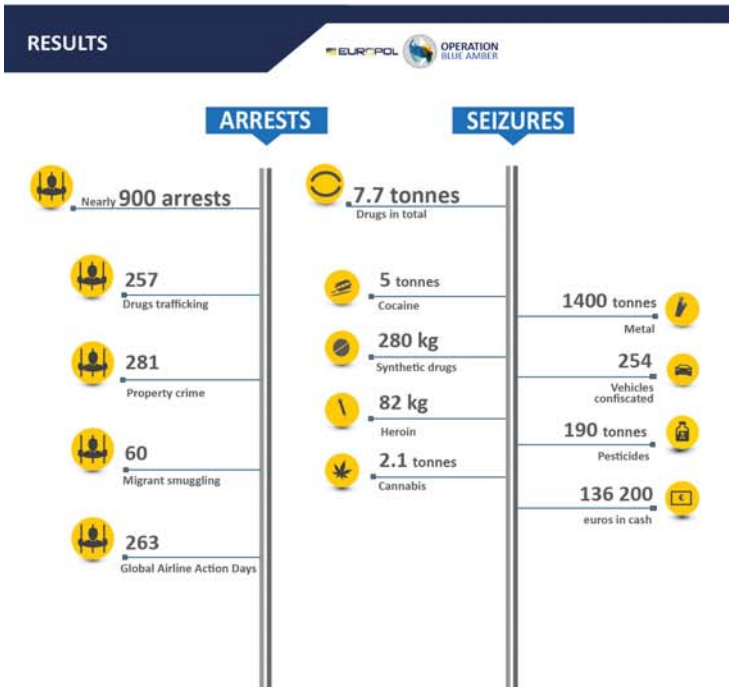
[23] European Multidisciplinary Platform against Criminal Threats (EMPACT): https://www.europol.europa.eu/content/eu-policy-cycle-empact

24/7 operational coordination centre

Liaison officers from the EU Member States and colleagues representing other international partners coordinated the exchange of information and intelligence between national law enforcement authorities from a 24/7 operational coordination centre at Europol’s headquarters in The Hague. Europol specialists and analysts provided support from its headquarters and also on the spot in EU Member States. Europol also facilitated the information flow between EU Member States, third states, various cooperation networks, international organisations and representatives of the private sector. Moreover, Europol supported Operation Blue Amber operations by deploying its officers on the spot in various locations, with mobile offices allowing for direct, secure access to Europol's centralised databases and analysis tools.


PARTICIPATING COUNTRIES
EUROPOL
OPERATION BLUE AMBER
EU Member States
Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Estonia, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxemburg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, United Kingdom
Third partners:
FRONTEX
INTERPOL
Australia, Albania, Bolivia, Bosnia-Herzegovina, Brazil, Canada,Colombia, Costa Rica, Dominican Republic, Ecuador, FYROM, Guatemala, Hong Kong, Iceland, Indonesia, Malaysia, Mexico, Montenegro, New Zealand, Nigeria, Norway, Panama, Peru, Philippines, Qatar, Serbia, Switzerland, Thailand, Turkey, United Arab Emirates, USA


OVERVIEW OF ACTIONS
EUROPOL
OPERATION BLUE AMBER
OPERATION TURNSTONE
DRUGS ACTION DAYS
OPERATION LUXCAR
OPERATION VOYAGER
OPERATION SIROCCO
GLOBAL AIRPORT ACTION DAYS 2
4/8 May
29 May
15/19 June
23/24 June
30 Sept/01 Oct
02/06 Nov
04/06 Nov
27 May
1/3 June
16/17 June
21/25 Sept
01/04 Oct
04/05 Nov
16/27 Nov
METAL THEFT ACTION DAY
GLOBAL AIRPORT ACTION DAYS
OPERATION VULCANO
OPERATION HIT 2
DRUGS ACTION WEEK
OPERATION MAUPIE


RESULTS
EUROPOL
OPERATION BLUE AMBER
ARRESTS
SEIZURES
Nearly 900 arrests
257
Drugs trafficking
281
Property crime
60
Migrant smuggling
263
Global Airline Action Days
7.7 tonnes
Drugs in total
5 tonnes
Cocaine
280 kg
Synthetic drugs
82 kg
Heroin
2.1 tonnes
Cannabis
1400 tonnes
Metal
254
Vehicles confiscated
190 tonnes
Pesticides
136 200
euros in cash

Two week focus on drugs trafficking yielded the seizure of 300 kg synthetics

Operation Blue Amber also included two drugs action weeks. Synthetic drugs trafficking and the use of small postal parcels to traffic the drugs is a key issue for many European countries. “During the Blue Amber drugs action weeks, the focus was specifically on this modus operandi of trafficking. In total, nearly 300 kg of synthetics were seized in and outside the European Union,” says Johan Nooijens, Chief Inspector of the Netherlands’ National Police Agency, and co-driver for ‘Empact Synthetic Drugs’. “The joint action days (JADs) on drugs were successful for us. The international information exchange and coordination is the key to success against these types of international organised crimes. Under the upcoming Dutch Presidency, joint action days on drugs will be organised and strongly supported again.”

250 stolen vehicles seized in operation Luxcar

The Luxembourg Presidency of the Council of the EU organised Operation Luxcar, focusing on vehicle theft. “More than 250 stolen vehicles were seized in a two-day international coordinated action, several new investigations were initiated with the support of many police officers in the EU and the support of Europol’s experts,” says Steve Schmitz, the coordinator of Luxcar for the Luxembourg Police. Property crime, and more specifically vehicle crime, continues to affect EU citizens.

Property crime in the EU
Organised crime groups commit property crime across the entire EU which includes organised vehicle theft, burglaries, armed robberies, metal and cargo theft. Relatively low punishments for most property crimes, their diversity and the fact that these crimes are often only investigated on a local level, make them attractive to criminal groups.

Property crime targeted in 80 000 checks on the Baltic Sea ferries

[Chart: operation presented in form of info-graphics]

Operation Turnstone, carried out in May 2015, targeted serious cross-border organised property crime[24] in the Baltic Sea region. Nearly 80 000 entities from passenger and vehicle lists of ferries operating across the Baltic Sea were checked both in the national and Europol databases, which triggered 325 hits on high-value targets. Four Estonian nationals were caught red-handed while attempting to break into a jewellery store in Norway. The offenders were arrested after an intensive surveillance operation which monitored the suspects from their initial arrival in Stockholm, by ferry from Tallinn, across more than 1000 km through Sweden to the city of Bodø in Norway.

Results:

10 operational action weeks (one financed by Europol), 7 days a week

Participating states: Estonia, Finland, Latvia, Lithuania, Norway and Sweden

EUR 2.5 million worth of items seized

200 suspects arrested

2000 intelligence hits

Lennart Ericsson, Operational Leader, Stockholm Border Police: “We coordinated an intense surveillance operation over 1000 km, from Estonia, through Sweden to Norway. Norwegian police apprehended the four suspects when they attempted to break into a jewellery store. The whole operation was led from Europol's coordination centre. The cooperation with Europol has been the absolute key to success for the operation Turnstone. Together we have created a common intelligence picture of the current situation in the Baltic Sea region. The continuous support from Europol has generated a large number of apprehended criminals within the framework of the project.”

[24] Target: suspects in the area of property crime, e.g. warehouse and shop burglaries (equipment, electronics, jewelry), vehicle and boat thefts, pickpocketing (organised groups), credit card skimming, metal theft.

1400 tonnes of metal seized

Also in May 2015, 17 EU Member States and Norway engaged in operational actions targeting key hotspots for metal theft and fencing of stolen metal. Overall more than 100 000 people and 30 000 vehicles were checked throughout the participating countries.

Results:

- 1400 tonnes of metal were seized (copper, iron, aluminium and non-ferrous metals);
- 191 people were arrested;
- 235 vehicles confiscated.

Cyprus: Two containers with illegally obtained cables were intercepted, which were from the UK and on their way to Pakistan

Spain: A Romanian organised crime group involved in copper theft was dismantled, with eight suspects arrested and three tonnes of copper seized.

Ireland: 400 000 beer kegs with a replacement value of approximately EUR 40 million had been stolen since 2007; numerous house searches were conducted, six suspects arrested and 282 beer kegs seized.

190 tonnes of pesticides seized

Law enforcement officers from Belgium, France, Germany, Italy, the Netherlands, Slovenia and Spain supported by private industry, joined efforts to target the illegal import of pesticides. As a result, 350 inspections were carried out in the seven countries and irregularities were found in 100 cases. In total, 190 tonnes of illegal or fake pesticides were seized. Such products may involve risks and hazards for humans, animals and the environment. Investigations are still on-going in seven cases.

24 facilitators of illegal immigration arrested

The Western-Balkan route plays an important role in the activities of people smuggling networks spread all over Europe. A targeted operation involving law enforcement officers from 11 countries, and Police Cooperation Convention for Southeast Europe Secretariat (PCC SEE) was launched against international organised crime groups involved in facilitation of illegal immigration in Southeast Europe. The two-day operation Sirocco led to the discovery of a safe house and the arrest of 24 facilitators. The operation also contributed to obstructing the secondary movements of irregular migrants from Central Asia to the European Union.

Long-term commitment to fighting organised criminal networks

Rob Wainwright, Director of Europol, summed up operation Blue Amber by saying that “criminals do not take borders into account and they need to know that they are no longer safe anywhere. It is our duty as law enforcement agencies to continue this international cooperation to tackle organised crime. Europol is committed to supporting national law enforcement agencies with its unique intelligence and technical capabilities.”

Joint action days (JADs) are cross-border law enforcement operations focusing on horizontal key crime hot spots and criminal infrastructures across the EU. JADs are a Member States-led initiative, supported by Europol, and take place within the EU Policy Cycle for organised and serious international crime.

No hiding place for criminals

Juan Miguel Thiriat Tovar, Head of the Colombian Liaison Bureau at Europol, said that operation Blue Amber was a clear demonstration of successful teamwork, where law enforcement from different countries could work together to coordinate operations in Europe, Oceania and America. “The results were more than just obtaining good statistics, it was to exert a lasting impact on the different structures of transnational organised crime groups. It was to send a clear signal to the criminals: there is no hiding place for you.”

INTELLIGENCE

The Secure Information Exchange Network Application (SIENA) enables the swift and secure exchange of operational and strategic crime-related information and intelligence between EU Member States, Europol and cooperating third parties.

The Large File Exchange (LFE) solution enables the secure exchange of large files that exceed the size limit (50MB) of the Europol Secure Information Exchange Network Application (SIENA) when the need arises (for example sending an image of a hard drive or copy of a server).

SIENA IN 2015

39 868 cases were initiated[25]

Increase of 16% over 2014

86% of the new cases were initiated by EU Member States

11% by third parties

3% by Europol

Crime areas of new cases

23% of new cases were related to other crime areas

17% of new cases were related to drug trafficking

15% of new cases were related to fraud and swindling

9% of new cases were related to robbery

8% of new cases were related to money laundering and illegal immigration

[25] This number includes cases initiated by Police and Customs Cooperation Centres (PCCCs). In 2015, 39% of new SIENA cases were initiated by the PCCCs.

732 070 operational messages were exchanged (an increase of 21% over 2014).

On average **60 000** messages were exchanged each month.

667 competent authorities are configured in SIENA

with **5531** users (a 17% increase over 2014)

28 Member States and 34 third parties are connected to SIENA

(15 third parties connected directly and 19 third parties connected indirectly).

In 2015, Europol continued to roll-out SIENA to specialised and regional units, including counter terrorism units in the Member States and partners having operational agreements with Europol. The number of counter terrorism units with access to SIENA has more than doubled since the beginning of 2015. More than 30 counter terrorism units now have access to SIENA. A number of changes have been made to adapt SIENA to the requirements of counter terrorism units to exchange information bilaterally.

The efforts to develop SIENA as the default secure communication tool for counter terrorism units will continue in 2016, with an upgrade to allow the handling of EU confidential information (for sensitive information exchange, such as CT, anti-corruption etc.) and with the roll-out of SIENA for additional counter terrorism units from Member States and partners having operational agreements with Europol.

The Europol Information System (EIS) stores information about offences, individuals involved and other related criminal data.

295 374 objects in the system (an increase of 25% compared to 2014)

86 629 suspected criminals (an increase of 40% compared to 2014)

633 639 searches were performed in the EIS in 2015 (an increase of 62% compared to 2014)

28 Member States (and Europol on behalf of the third parties) are using the EIS which equals to 4569 users

Major crime areas related to objects:

26% related to robbery

20% related to drug trafficking

7% related to illegal immigration and other offences

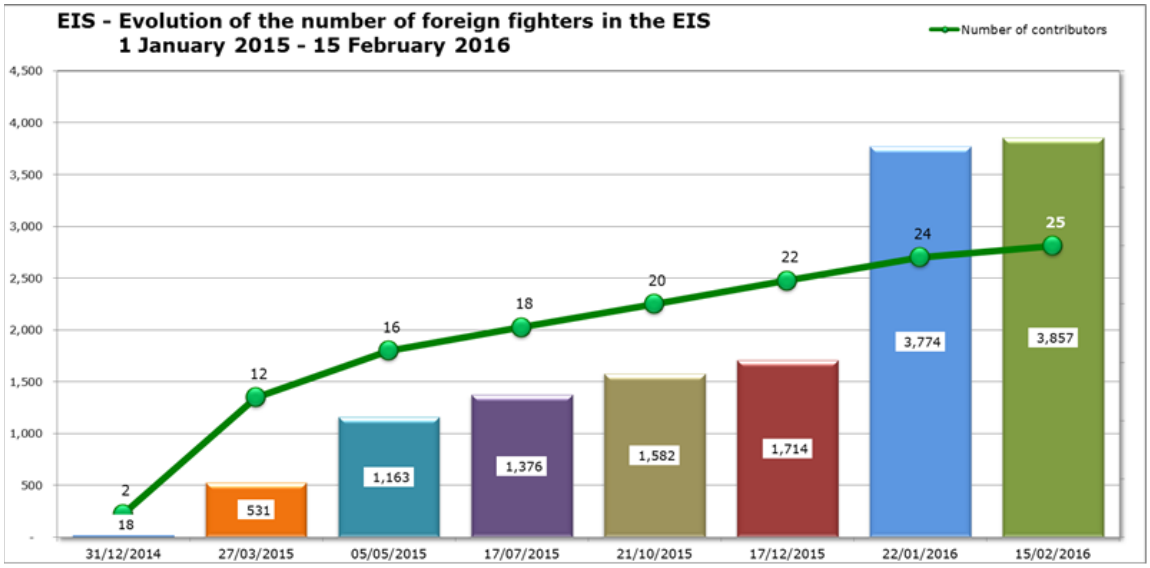
6% related to fraud, swindling and money laundering

5% related to forgery of money

Year	EIS: Number of objects
2010	174 459
2011	183 240
2012	186 896
2013	245 142
2014	249 797
2015	295 374

Intelligence on foreign terrorist fighters

Europol and several Member States proposed a ‘three-tier intelligence gathering’ approach to create synergies and improve intelligence gathering and sharing by the simultaneous use of the Schengen information System (SIS II), Europol Information System (EIS) and the specialised analysis project at Europol on foreign terrorist fighters (FTFs). As a result, 24 countries and organisations used the EIS in 2015 to share lists of foreign terrorist fighters. Remarkably, by the end of 2015 around 20 counter-terrorism units had direct access to the EIS, allowing them to consult the system directly. Another positive development was the increased number of hits on terrorism during 2015 which, on several occasions, led to joint law enforcement actions between various countries.



100 analysts looking for trends, patterns and missing links

The Europol Analysis System (EAS) is the state-of-the-art and powerful analysis tool supporting Europol analysts in the operational and in-depth strategic analysis of data provided by Member States and third parties. It provides a technical platform hosting analysis work files. The EAS contains integration points with other core information processing systems at Europol such as SIENA and the Europol Information System.

More than 100 analysts are employed at Europol. They perform operational and strategic analysis and work for dedicated projects within the area of organised crime and terrorism. Analysts are also employed in Europol's Operational Centre, which is staffed 24/7. This unit manages the constant flow of data between Europol and its operational partners, assesses the data to be included in Europol databases and supports law enforcement operations across the EU and beyond. Europol's Operational Centre maintains a centralised cross-checking service and produces analytical reports when common elements are found.

NETWORKS

More than 8000 experts connected via the Europol Platform for Experts

The Europol Platform for Experts (EPE) is a secure collaboration web platform for experts in a variety of law enforcement areas. It facilitates the sharing of best practices, documentation, innovation, knowledge and non-personal data on crime. This is the only Europol core system that does not support the exchange and storing of personal data and classified information. Users can interact and collaborate with each other via virtual communities. Each community comes with a set of tools for content management such as a blogs or forums, and communication, such as private or instant messaging.

By the end of 2015, 8140 users from 84 countries could interact and collaborate with each other in virtual communities. In 2015, approximately 2000 new users joined the EPE, which is an increase of 35% compared to 2014.

Top 3 communities in terms of number of users

- **The Secure Platform for Accredited Cybercrime Experts**
  2100 registered members – almost double compared to 2014: the Secure Platform for Accredited Cybercrime Experts allows specialists from a variety of law enforcement areas, the private sector and academia to share knowledge, expertise, best practices and non-personal data on cybercrime.
- **The Financial Crime Information Centre**
  1200 registered members: the Financial Crime Information Centre platform provides a support service to investigators and judicial authorities by collating information from various sources on financial crime that might be relevant for practitioners in their daily work. It focuses mainly on money laundering and asset recovery.
- **Intellectual Property Crime**
  600 registered members from academia, law enforcement and private industry: the purpose of this platform is to develop strategic analytical knowledge and best practices on intellectual property criminality and counterfeit products.

700 EU explosives and CBRN specialists share intelligence

The EU Bomb Data System (EBDS) provides a platform for the timely sharing of relevant information and intelligence on incidents involving explosives, incidents related to explosive ordnance disposal (EOD), and chemical, biological, radiological and nuclear (CBRN) materials. Over 700 experts from almost all EU Member States, Europol, Norway and the United States are already connected and using the system. Cooperation among CBRN specialists is facilitated by the European Explosive Ordnance Disposal Network. Experts meet at least once a year to compare their respective protocols. This work is highly important for responding to incidents with cross-border aspects.

Whenever an EOD/CBRN-related incident occurs anywhere, national specialist units start the long process of gathering the necessary technical intelligence and information on that incident, which will ensure they are up-to-date on the latest terrorist and criminal developments in this area, as well as the measures used for countering them. Thanks to the EBDS, Europol can provide instant access to existing related information.

Europol Liaison Officers

More than 190 liaison officers representing EU Member States and third countries are present at Europol to facilitate cooperation and information exchange between states and their national services and Europol.

SIMON RIONDET

Head of the French Liaison Bureau since 1 September 2015

Born:	Lyon, Rhône
Most recent location:	Martinique (French West Indies)
Education:	MA in Law and Security Policy, MA in Defence and Security
Work experience:	17 years
Specialisations:	Organised crime, drugs trafficking, special surveillance and intervention techniques, international police cooperation

Simon was appointed head of the French Liaison Bureau on 1 September 2015. September was a very active period for the heads of law enforcement agencies in Europe but also other partner states, with the 2015 European Police Chiefs Convention (EPCC) plus operational meetings within the framework of operation Blue Amber action days.

Simon finds it challenging but extremely rewarding to work in an international environment on combating cross-border crime. For Simon, “Europol provides not only some of the finest tools to support criminal investigations (state-of-the-art databases, secure information exchange, strategic and operational analysis), but it is also a unique place where almost 200 liaison officers from 38 states are able to connect in a minute to deal with serious and organised crime.”

The Paris attacks on 13 November 2015 intensified France’s cooperation with Europol on counter terrorism matters. The excellent flexibility of the agency was demonstrated by setting up the Emergency Response Team less than two hours after the terrorist attacks, and providing great live support to the French and Belgium investigations. “This has also shown that Member States stand united when facing a common threat. All countries have provided fast and accurate support to handle the terrorist attacks. The use of Europol’s tools, such as SIENA to enable the international exchange of data, reached an unprecedented level,” says Simon. In general, the use of Europol’s resources is constantly increasing. France opened 3000 new cases at Europol in 2015 and exchanged a total of 42 000 messages. This growing trend is also seen among other EU Member States and cooperation partners.

Simon notices that “Europol is not only an agency which provides the state-of-the-art analysis capabilities and information and intelligence sharing tools. It is also a place where a united Europe becomes a reality. I would like to underline the numerous signs of solidarity and support coming from colleagues representing various states and also from Europol officers. This leads me to the conclusion that Europol is about a mind-set: a wish to effectively cooperate against terrorism and serious and organised crime and a wish to stand united against the multiple and increasingly complex threats to our internal security.”

ERIC STROM

FBI Liaison Officer to Europol since 21 May 2015

Born:	Chicago, Illinois
Most recent location:	Pittsburgh, Pennsylvania
Education:	JD in Law, MA in Technology Management, BA in History
Working experience:	17 years
Specialisation:	Cybercrime (10 years), organised crime (7 years)

Meet Eric, the FBI's first permanent liaison officer to Europol. Over the last decade, Eric has developed expertise in creating and managing public-private partnerships focusing on disrupting and dismantling numerous cybercriminal organisations responsible for sophisticated cyber attacks against the US and EU Member States. Eric reported for duty at Europol in May 2015 and will be assigned here for at least three years. While Eric was initially assigned to work within the Joint Cybercrime Action Taskforce (J-CAT), he has worked hard to broaden the FBI's presence in both the counter terrorism and organised crime units.

"With the arrival of FBI Director James Comey, the FBI has looked at ways to better leverage multi-lateral relationships in intelligence dissemination, case, coordination and de-confliction," says Eric. He believes that Europol provides the perfect platform for this: "Having worked in an active public-private sharing environment over the last decade, I greatly appreciate the positive sharing environment that Europol has established. The dedication and team atmosphere here is terrific."

Eric points to the recent Darkode cybercriminal forum takedown this past summer as a great example. "Darkode was an FBI led investigation that had members located across the globe. Europol's European Cybercrime Centre provided a critical platform that assisted the FBI in analysing and developing target packages, hosting multiple coordination meetings as well as establishing the primary command post to track the global law enforcement effort on the takedown action day."

Aside from his normal work duties, Eric has also been busy coordinating the recent visits to Europol by both the US Attorney General Loretta Lynch as well as FBI Director James Comey.

LOOKING FORWARD

LUIS DE EUSEBIO RAMOS

DEPUTY DIRECTOR

CAPABILITIES DEPARTMENT

As the new Deputy Director responsible for the Capabilities department, I arrived in August 2015 to see a dynamically developing organisation facing multiple new challenges and expectations related to the European security situation.

The year 2016 will present a number of new challenges and opportunities. With the new Europol Strategy coming into force and the ongoing work on the draft Europol Regulation, the Capabilities department will enter a new phase whereby it needs to become even more flexible and have a stronger core business orientation.

With regards to human resources management, one of my main priorities is to ensure that staff members are properly engaged, especially in view of pressing operational priorities and Member States' needs. This year a new Human Resources Business Manager will be appointed, who will address sensitive matters such as staff mobility, recruitment, and job architecture.

The increasing number of staff remains a challenge for the administration, notably in the areas of accommodation and infrastructure. This year we will present and start implementing the Strategic Housing Roadmap in order to get the best from the available workspace while maintaining the highest quality level of working conditions for Europol's staff. More operational focus and thus more staff will also mean increased budget, which will have to be administered in an accurate and sound way in line with our priorities to support EU Member States.

In the ICT area, 2016 will be a year of consolidation of our core systems, especially SIENA and the Europol Analysis System, and preparation of the technological infrastructure for the upcoming implementation of the Integrated Data Management Concept. The main objective will be to upgrade the existing systems and develop the Universal Message Format allowing for an easier and more structured cross-border communication exchange of criminal-related data.

I have a strong belief in Europol's mission and I am convinced that in cooperation with the whole team we will succeed in overcoming the challenges and make 2016 yet another dynamic and inspiring year for Europol.

OLDŘICH MARTINŮ

DEPUTY DIRECTOR

GOVERNANCE DEPARTMENT

Being in the centre the EU security architecture, Europol is constantly upgrading its processes and capabilities to provide effective and timely reactions to evolving security threats. 2015, in particular, was a year of significant and rapid developments in the areas of terrorism and migration. Europol had to react promptly to the new security challenges and focus its resources on the pressing operational needs. November's terrorist attacks in Paris required many Europol officers, including those in the Governance department, to be permanently available ensuring smooth communication within and outside the organisation and supporting the agency's operational units.

As of 2016, Europol is working on the basis of its newly adopted Strategy for 2016-2020. In the next five years, Europol's core purpose and focus will remain unchanged. We will concentrate on consolidating all capabilities and expertise to deliver the most effective support for Member States' investigations. The strategic emphasis of the organisation will be placed on the full-scale delivery of operational services and operational impact.

The Governance department will continue its efforts to ensure a smooth transition to a new legal basis. The close of year 2015 brought political agreement on the new draft Europol Regulation. The final plenary vote of the European Parliament is foreseen for May 2016. Once the legal text has been approved by the European Parliament, the implementation of the new Europol Regulation will commence. This will affect all departments at Europol. The new legal framework is expected to be applied as of mid-2017.

Other priorities will include cooperation with relevant third countries and bodies, delivery of centralised procurement support to all departments, and addressing current security threats to further improve existing security arrangements of the organisation.

WIL VAN GEMERT

DEPUTY DIRECTOR

OPERATIONS DEPARTMENT

In the last year's review we focused on the trend of increasing information flow; the trend which, in fact, was even stronger than expected, resulting in an increase in every field of support given by Europol. A significant milestone was reached by December 2015 with 600 000 searches performed in the Europol Information System, reflecting an overall increase of more than 60% in the use of the system. This shows that Europol, although stretching its current resources to maintain this trend, is a crucial hub for criminal information exchange and analysis in Europe.

The migration problem, the trends in organised crime and also the terrible terrorist attacks made it clear that a stronger pan-European approach is needed. To respond to this need, Europol and its Operations department will adapt. In line with the new Europol Strategy for 2016-2020, focus will be given to direct operational support and analytical work. By using the positive experience of bringing the support together in a centre-like approach as was previously done with the European Cybercrime Centre, Europol will support Member States even more by opening the European Counter Terrorism Centre and the European Migrant Smuggling Centre in 2016. Together with a new approach on data handling and creating 24/7 support for Member States, Europol will be able to present its services in an even more timely and direct manner. By using the European Union Regional Task Force concept and related investigative and analytical support on the spot, we will provide more direct support to law enforcement in the Member States.

Delegation agreements, joint action days and more operational cases, and increasing cooperation with our partners within law enforcement and private sector partners where relevant, will still be part of our ongoing efforts to make Europe safer. Speaking on behalf of Europol's Operations department, I can say that we are very proud to be contributing to this goal.