

A PERSPECTIVE ON SUPPORTING AN INVESTIGATION BY EUROPOL

Michal Otrebski
The Representative of Poland
In EUROPOL

Europol is the European Union law enforcement organization that handles criminal intelligence. Its aim is to improve the effectiveness and co operation between the competent authorities of the Member States in preventing and combating serious international organized crime. The mission of Europol is to make a significant contribution to the European Union's law enforcement action against organized crime, with an emphasis on targeting criminal organizations. The Europol Convention states that Europol shall establish and maintain a computerized system to allow the input, access and analysis of data. The Convention lays down a strict framework for human rights and data protection, control, supervision and security.

The Europol Computer System will have three principal components:

- I. an *information* system;
- II. an *analysis* system;
- III. an *index* system.

The analysis and index systems are already in place. The information system is under development and is planned to be operational in the nearest future.

The Joint Supervisory Body, comprising two data protection experts from each Member State, monitors the content and use of all personal data held by Europol. Europol is accountable to the Council of Ministers for Justice and Home Affairs. The Council is responsible for the guidance and control of Europol. It appoints the Director and the Deputy Directors and approves the budget. All Member States have their representatives in the Council of Ministers, and the requirement for unanimous decisions helps ensure a democratic control of Europol. The Europol Management Board comprises one representative from each Member State, and has the overall task of supervising the activities of the organization.

Based on Article 30 of the Amsterdam Treaty and on the European Council summit in Tampere, Finland 1999 the following developments have either taken place or are under construction:

- By Recommendation of 29 September 2000 the Council requested that the Member States “should deal with any request from Europol to initiate, conduct or co-ordinate investigations in specific cases and should give requests in due consideration. Europol should be in principle informed whether the requested investigation will be initiated and of the results of any such investigation.”
- By Council Act of 30 November 2000 the competence of Europol was extended to include money laundering in general, regardless of the type of

offence from which the laundered proceeds originate. This amendment of Europol's Convention has to be ratified by all Member States following their constitutional requirements. This process has already been initiated.

- By Recommendation of 30 November 2000 the Council asked Member States, with due regard to the Europol Convention and to its implementing rules, to make full use of the possibilities for Europol support for joint investigative teams. Europol will through the Europol National Units (ENUs) provide support to the joint investigative teams in accordance with the Convention especially for the following purposes and according to the following arrangements:
 - Place Europol's knowledge of the criminal world at the disposal of joint investigative teams.
 - Assist with co-ordination of operations by joint investigative teams.
 - Provide advice to joint investigative teams on technical matters.
 - Help with the analysis of offences.
- The European Police Chiefs Operational Task Force took up its activities. Its aim is to exchange, in co-operation with Europol, experience, best practice and information on current trends in cross-border crime and contribute to the planning of operations.
- Preparatory work for the establishment of an European Police Academy has been started.
- The European Council summit in Nice, France on 9 December 2000 agreed upon further steps for Eurojust. Complementary to Europol it should be composed of national prosecutors, magistrates, or police officers of equivalent competence, detached from each Member State according to its legal system. Article 31 of the Treaty of Nice stated: "The Council shall promote co-operation through Eurojust by:

promoting support by Eurojust for criminal investigations in cases of serious cross-border crime, particularly organized crime, taking account, in particular, of analyses carried out by Europol;..."

1. Databases

The Interim Information System (IIS) has been renewed and delivered and it has been used by the Core Group to store data in expectation of the EIS. After the events of 11 September, a Counter Terrorism Support System, aimed at storing data related to terrorism without dissemination throughout the Europol network, was built based on the IIS architecture. This system can currently handle very sensitive data.

The business rules, functions and roles to be applicable for the use of the IIS have been specified and validated, including a user manual.

Version 0.1 of the Europol Information System (EIS), containing the main functionality related to combating the counterfeiting of the Euro, was declared deployable on 30 December 2001. It is expected that version 0.1 will be in use at the nearest future.

The business rules to be applied for the use of EIS have been specified, validated and published on the Intranet. The policy on the use of EIS has been described and presented to the Heads of Europol National Units, the Project Board, and the Intelligence Experts.

In addition, in order to allow the integration of the Information System in the Europol environment, the Windows NT based server infrastructure has been upgraded to Windows 2000, including the modification of hardware where necessary.

The new version of the Index System, which comes closer to the expectations of the users, has been delivered and subject to the advice from the Joint Supervisory Body will be made operational.

The modification of the Info-Ex (Europol's computerized tool for secure exchange of information and intelligence) application started in order to integrate the new mandates and the Task Force as a user group. The objective to modify the application in function of the new mandates was not entirely achieved, as problems with backward compatibility of different versions of office software packages were detected.

In order to permit Third States to have a secure technical link with Europol, a new network, physically separated from the Internet and the Europol Network has been created, using ISDN links and encryption devices.

A new concept of the Analysis System (Eurint) to include the pre-processing of information was developed and used as an interim solution. It will be the basis for the development of the new system, the Overall Analysis System for Investigation Support (OASIS). A requirement analysis of this new analysis system was started and largely completed in 2001.

The Virtual Private Network (VPN) was tendered for and was implemented in all Member States, in conjunction with the encryption devices and its management hardware and software.

A new Security Application has been delivered, containing new functionality and allowing the client to run software on a Windows 2000 workstation.

Together with potential in-house users, Europol Research Unit tested and evaluated externally developed technology, dealing with cybercrime research, multilingual terminology, forensic computing, knowledge discovery, graphical representation, natural language processing and security.

2. Analyses

A total of 16 Analysis Work Files were run and 29 Operational Analysis Reports were produced based upon the data provided by Member States and in some cases Third States. Other products such as Interim Reports, Monthly Update Reports and Strategic Assessments supplemented this, including 25 Strategic Reports. Emphasis has been given to the development of threat and risk assessments rather than general situation reports, in order to assist in operational decision making.

In 2001 The approach to Analysis Work Files projects has shifted from a very generic to a more target-oriented approach. This approach also affected the provision of data relating to ongoing investigations from the participating Member States.

More importantly the output has led to results for investigations in Member States, and a direct consequence has been the identification of targets, arrests and the development of new cases, some involving Third States.

Work was devoted to the development of four new Analysis Work Files projects, such as child pornography and money laundering related suspicious transactions. Analytical activities on four Analysis Work Files were ended during the year either due to the operational objectives being met or because intelligence suggested that these were no longer viable.

On request Europol provided analytical expertise to seven Member States operational projects with Europol Support linked to ongoing investigations in the Member States. This support resulted in an additional 24 Operational Analysis Reports, leading to target identification, understanding of criminal networks, enhanced co-operation between investigative units, improved collection of intelligence and evidence for criminal cases and finally arrests.

Europol continued the development of the European Union Organized Crime Report for the year 2000. As planned both the closed and open versions of the Europol 2000 Organised Crime Situation Report were distributed.

Analytical support was given to the production of assessments on Ethnic Albanian Organised Crime and West African Organized Crime. Further activities were devoted to the development of the strategic assessment related to Cybercrime.

A total of 18 internal analytical reports were produced in relation to emerging trends, events and new phenomenon that either required urgent action or were related to the extension of the mandate.

Operational analysis training courses were provided on request to three Member States and one Third State (Slovenia). Following on from Operational Analysis training given in previous years Europol continued to support the Joint UNDCP-PHARE programme for strengthening drug law enforcement capacities in Southeast Europe for Bulgaria, Former Yugoslav Republic of Macedonia and Romania.

Europol continued to promote awareness of intelligence analysis within law enforcement.

3. Co-ordination

The Task Force's first products were the European Union Threat Assessment Document on Islamic Extremist Terrorism and the first European Union overview on security measures in relation to terrorism. Furthermore the Europol bomb database, already created by Europol before 11 September, was put at the disposal of the Task Force. This database includes technical details of explosive devices. Other Task Force activities include the assessment of the financing of terrorism, with a view to undermining terrorist activity by seizing its funds or assets, and the procurement of an Arabic-to-English translation system for the evaluation of the large amount of intelligence in Arabic transmitted by Member States to Europol.

On 11 September an Operational Centre was created, which gives a 24-hour service in the exchange and co-ordination of information and intelligence, and produces daily briefing papers.

Notwithstanding the disruption of priorities as a result of 11 September, Europol provided several products and services related to counter-terrorism.

The exchange of counter-terrorism information between Member States via the Europol Liaison Officer and National Unit networks grew. A special

conference on Terrorism was held in Madrid from 29 January to 2 February 2001.

Several directories were updated, e.g.: counter-terrorism responsibilities at national level within each Member State; counter-terrorism legislation in Member States; Counter Terrorism Competencies/Centres of Excellence in the Member States.

The Open Source Digest on terrorism related activity was disseminated to the Member States on a weekly basis. Also updated was the Glossary of terrorist groups containing basic details about their origins, ideology/objectives, leadership and activities.

Periodical trend and situation reports on topics related to terrorist crime, based on open source information and reporting by Member States to Europol.

In 2001 two Analysis Work Files within the area of CT competence were continued. Due to the 11 September attacks, one Analysis Work File increased in importance and produced output with added value to Member States.

4. Technical support

Information exchanged with the investigation teams, several operational meetings, operational analysis and co-ordination support resulted in the furthering of national investigations. In turn several arrests; seizures of drugs, weapons and financial assets have initiated several new investigations.

A European Union situation report on East European organized crime in 1996-2000, a threat assessment on East European organized crime 2000 and a threat assessment on Russian organized crime 2001 were disseminated to the Member States. The Analysis Work File resulted in the identification of seven targets and led to Law Enforcement actions in the respective Member States.

New initiatives on other organized crime groups – e.g. West African groups – were started.

Future co-operation was outlined in relation to cybercrime covering matters such as the creation of a network of cybercrime units, the implementation of a monitoring centre at Europol, the improvement of intelligence gathering and the setting up of working group with the private sector.

The development of a common approach for the Witness Protection Program progressed.

In the field of technical support, activities focused on raising awareness and providing expertise and advice.

Tests on specific devices were conducted throughout the year 2001, the results of which were subsequently reported to the national technical support units.

On request, four training sessions of one week each were provided to Member States concerning the use of specific technical surveillance devices.

A series of draft guidelines on how to handle informants were drawn up aimed at developing standards and enhancing co-operation and information exchange.

The Manual on Best Practices and Techniques related to Police Investigations in the European Union and the Manual on Controlled Deliveries were updated with Member States' contributions both on CD-ROM and on the Europol Intranet.

5. Examples of the results achieved on the export controls in Europe

Nuclear material

Currently very few cases in the European Union and Eastern Europe involve weapon-grade fissile material. The cases that we are aware of are seizures of a few grams of HEU, or plutonium sources.

This is a short overview of the most recent cases:

On 26 January 2001, acting on a tipoff, 245 static eliminators coated with a total of two grams of Plutonium 239 were found by the Greek police, buried in a forest near Thessaloniki. Apparently it was produced by Mayak in Russia and smuggled through Bulgaria. We are not aware of any arrest in this case.

On 6 July 2001, the theft of Plutonium-contaminated waste was detected at the decommissioned fuel reprocessing plant in Karlsruhe, Germany. A German national who was working at the facility has been recently sentenced in this case. The quantity of plutonium was less than one milligram, but the perpetrator and his girlfriend have suffered serious contamination. Decontamination of their apartment and car have involved a 2 million € cost for the German authorities.

A much more relevant case occurred in 16 July 2001 in Paris. Police seized a 2,5 grams sample of enriched uranium at more than 72%.

Analysis conducted by the CEA have shown that the material consisted of reprocessed spent fuel of Russian origin. It has now been ascertained that the material had transited via Romania and Moldavia. So far, nationals from Romania, France, Portugal and Cameroon were identified as being involved in the smuggling network, which appeared to be well-organised and functioned for possibly several years. A trial in Paris is expected next year.

The material seized in Paris is extremely similar to the 4 gram sample seized in Bulgaria in May 1999, and analysed by the *Lawrence Livermore National Laboratory*. The Bulgarian investigations show the same links to Romania and Moldavia. So far the Russian facility from where the HEU was stolen still needs to be identified. No criminal organization could be identified in this network, mostly composed of individuals who were also running legal businesses.

On 15 May 2002, one hundred smoke detectors fitted with plutonium sources of Russian origin were seized in Bulgaria, and four smugglers arrested.

In addition, one can mention the theft of two smoke detectors with plutonium sources from the Ignalina nuclear power plant in Lithuania in June 2002.

We are not aware of any other recent case in Europe for the past two years.

A few more cases involve low-enriched, natural or depleted uranium.

We have kept an interest in the situation at the research reactor of the Kinshasa University, as a fuel rod stolen from this facility was seized by the Italian police in 1998. Recent reports mention the possibility that another rod, containing about 2 kilograms of uranium enriched at 20% also disappeared.

From our perspective, the only worrying case is the Romania-based one, as we do not know how many samples have been successfully smuggled in the past few years, and who the recipients were. Moreover, the exact origin of the material remains unknown to us. In addition, we know that the smugglers have been monitoring customs activity before crossing the borders, and that they have used efficient shielding containers to prevent radiation detection.

Besides this specific network, the other cases mentioned can be assessed as being of low interest from a non-proliferation perspective.

Radioactive substances

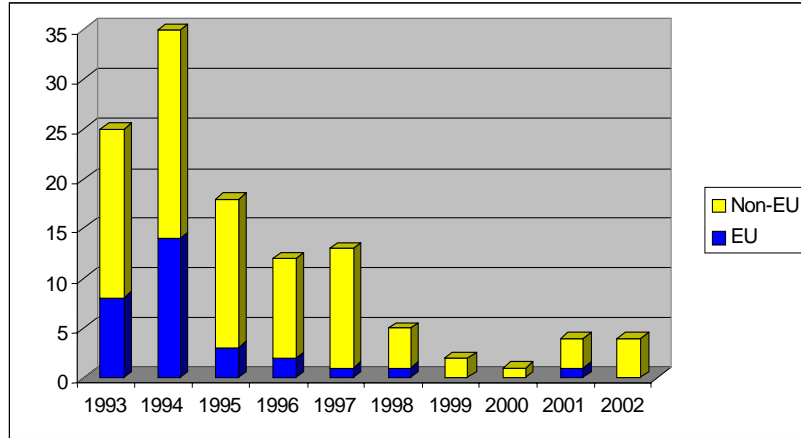
Many incidents involving radioactive sources have occurred in Europe in the past two years.

By far, the substance the most frequently involved is Caesium 137. Most of the cases concern thickness or moisture gauges, smoke detectors, sometimes more powerful sources used in radiography devices. However, most of them concern sealed sources of low activity, or metallic elements of little use in the making of a radiation dispersion device. We have also noticed repeated thefts of Iodine 125 sources for medical use in Italy; however these sources were of low activity and with a half-life of less than two months. Let's mention a case that occurred in March 2001 in Moscow: 268 grams of Cesium-137 were proposed for sale by three Russian nationals. However the Russian authorities have not confirmed the case. We are not aware of any other seizure of a significant quantity of radioactive substances in Europe.

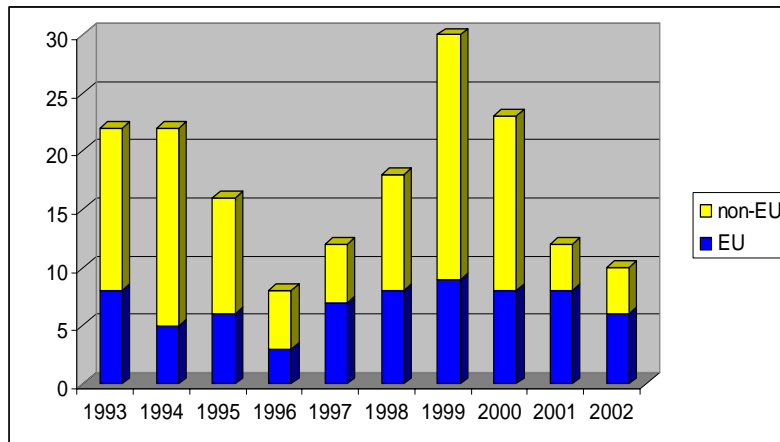
Findings from the cases

Taking into account that only a fraction of the illicit trafficking cases is uncovered by law-enforcement agencies, the main features of this issue are:

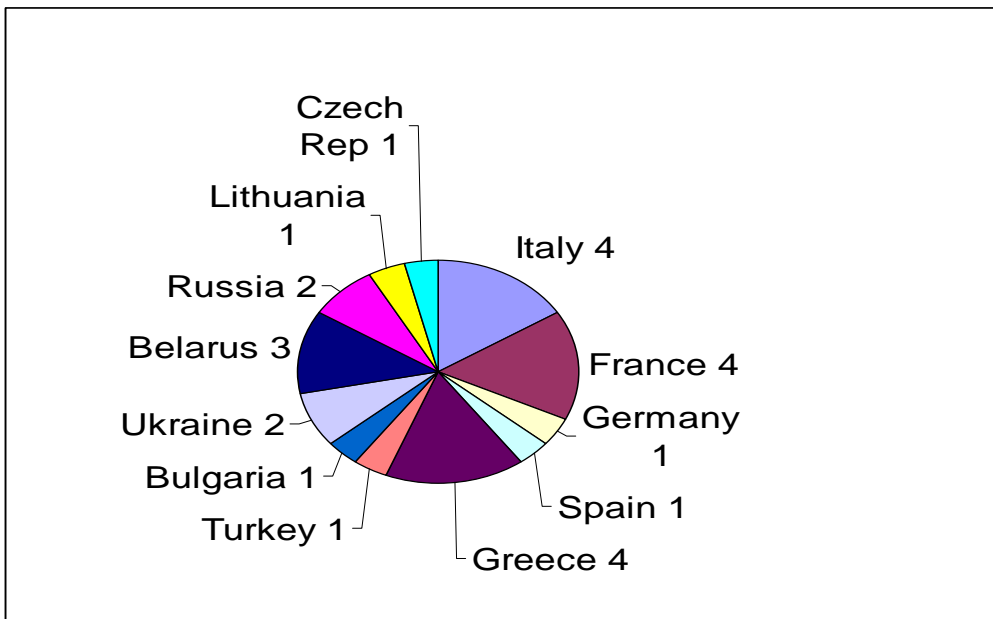
- The existence of an unbalanced black market. Motivated by the hope of easy money, insiders of nuclear or industrial facilities, aware of the weaknesses of the security measures, steal some sources. Usually they are sold to members of the local mafia, who also expect a benefit from the transaction. However, "end-user" clients are very scarce. As a result, sooner or later police or intelligence agencies often become aware of the proposal.
- The expected profit from the transaction is almost never met.
- The general absence of security concerns. Very often smugglers are not aware of the danger and receive high doses of radiation.
- When no client is found for a source, it is frequently abandoned anywhere and can cause environmental contamination or injuries to person(s) who find it.
- In some cases, criminal groups have used the same routes for smuggling radioactive substances and cigarettes, weapons or drugs. This is apparently the case in the South East of Europe.
- The vast majority of the cases are uncovered following intelligence received by law-enforcement agencies. The smugglers are usually aware of the existence of radiation monitoring devices at some border check points and avoid them. Very few cases result from border controls.
- There is no significant increase of the overall number of cases detected on the European continent.



Cases involving nuclear material (excepted depleted uranium) in Europe from 1 January 1993 to 1 September 2002



Cases involving radioactive substances (excepted unauthorized disposal and contaminated scrap metal) in Europe during the same period



Number of cases of theft, unauthorized possession or transfer of nuclear material and radioactive substances
In Europe
Period 1 January 2001 to 1 September 2002
(as reported to the IAEA or by the national regulatory bodies)

CONCLUSIONS

Europol is an relatively young organization. Both the databases or the operational methods are still being improved and developed. But there is no doubt that its role and importance will be growing in the nearest future.

I would like to emphasis that all mentioned above tools can be used by the EU member states in cases of any crime, which is consistent with the mandate of Europol. These possibilities obviously refer to any kind of crime, also related to the export controls.

The Analytical Work File may be established by each member state of EU. If any other state has an interest to join the AWF, participation is possible. Then the group of states start to collect intelligence. Non EU countries can support this activity.

All the files are proceeded by professional analysts. The effects of their work are available for all the participating countries.

For this purpose it is also possible t create Join Investigative Teams.

FOURTH INTERNATIONAL CONFERENCE ON EXPORT CONTROLS

WARSAW, POLAND

SEPTEMBER 30-OCTOBER 3, 2002

Each European Country may run an operation under the Europol's umbrella. In this case the organization provides co-ordination and technical support.

It's very important that the number of non EU countries and organizations, co-operating with Europol is systematically increasing. That means that Europol will be playing an increasing role in the effects achieved in combating international criminality.