THE 6th INTERNATIONAL SUMMIT ON TRANSNATIONAL CRIME
Monte Carlo - 13 – 15 October 2004

Plenary Session :

"COUNTERFEITING AND ORGANISED CRIME AND MAFIAS"
Thursday – 14 October 2004

Chairman: Dr. Marius – Eugen OPRAN
Adviser to The President of Romania

Your Excellencies,
Ladies and Gentlemen,

Concerning our debate, first of all it is necessary to identify the sectorial types of economic and financial crime, which our session should address. Without implying any order of priority, my proposal is to examine the following clusters of crime, being organized or non-organized:

- Corruption
- Fraud, notably with regard to product counterfeiting and piracy and the fraudulent use of non-cash means of payment
- Theft in the area of intellectual property
- Money laundering
- Major cybercrime issues

Very briefly, I want to outline some major aspects concerning the above-mentioned criminal activities:

► From the beginning, we should point out that the organized crime is a very flexible phenomenon. It would "always go where the money is and the least risk". This would require a flexible approach from the Summit with a view to encompass new trends.
► As regards money laundering, there is a need to differentiate between acts of money laundering committed by organized crime groups and those committed by individuals or companies.
► Concerning the area of counterfeiting and product piracy, I want to outline the importance of these areas for our session, because it is first

of all up to the trademark and copyright owners to protect their rights through preventive measures. Thus, national, European and international professional associations could supervise markets and new trends in counterfeiting and piracy by creating databases or cooperating with public authorities. This practice could be extended also to other public bodies, like customs authorities, police etc. We should outline also the importance of training measures or information campaigns.

► According with a study carried out by PWC, the issue of companies as victims of crime had become a growing concern among stakeholders. Whilst "good management" had recognized the need for effective in-house fraud prevention through more accountability and transparency in order to limit the reputation damage, many small and medium-sized enterprises still did not have any anti-fraud mechanisms in place. Others are concerned rather about profit making than expensive crime prevention. Also, there is a trend only to comply with law-imposed action such as in the field of money laundering. Voluntary measures on the other hand in the field of fraud prevention are still perceived like as a non-value cost. According with the same PWC study, corporate organizations did not want to share their bad experience because of fear for their reputation. Surprisingly, two thirds of crime-affected companies did not see the need to change their control procedures, which had apparently failed. Therefore, it proved difficult to persuade companies to introduce additional fraud prevention techniques. Cybercrime issues turned out to be an ever-growing concern for the companies.

► Concerning data protection, we should highlight that a balanced approach of respecting these rules on the one hand and allowing data collection for investigative and preventive purposes would be indispensable. As regards the need to respect legitimate interests of private sector, we are obliged to take into account the fact that some professional groups are not determined by profit making. Also, the specificities of all independent professions should be respected.

► The business community should be strongly recognized as a partner in crime prevention, working voluntarily mainly in three directions: applying business security practice and principles; issuing self-regulation in each commercial sector; adopting self-regulation code in a single corporation, which means an internal compliance system with ethical guidelines and control.

► More and more companies had to deal with infiltration of illicit activities on the one hand and higher expectation from consumers and the public opinion on the other hand to provide not only quality goods and services, but also to do this in a sustainable and ethical way. The private sector should try to meet these new trends with self-regulation mainly.

► Given the worldwide dimension of the Internet, safety and confidence in cyber-space is an activity which calls for a collective response on a global scale. Computer - related crimes are committed across cyber space and do not stop at the conventional state – borders. They can, in principle, be perpetrated from anywhere and against any computer user in the world. It is clear that activities that are unlawful off-line will not cease to be unlawful through going on-line.

► It may prove more difficult to protect individuals' rights in cases of cyber-crime because of complex issues such as the determination of the competent jurisdiction, the law applicable and cross-border enforcement. The treats are well known: child pornography, hacking, denial of service attacks, spread of malicious viruses, fraud involving electronic data, racism and promotion of xenophobia, infringements of intellectual property and illegal invasions of privacy. These threats need to be taken seriously. Protection of potential victims is a fundamental concern as well as trust in the reliability and security of networks, which is a pre-condition for take-up of the Internet and the birth of mass *"e-Commerce"* markets.

► The European Commission has already taken action to fight cyber-crime, launching a large debate at EU level between all different stakeholders involved and presenting a legislative package to approximate the specific areas of substantive criminal law in the area of high-tech crime.

► According with the Commission recommendations, can be emphasized that a comprehensive policy program to fight against cyber-crime should presuppose at least four key conditions:

- the adoption of adequate substantive and procedural legislative provisions to deal with both domestic and transnational criminal activities;
- the availability of a sufficient number of well-trained and equipped law enforcement personnel;
- the improvement of the co-operation between all actors concerned, users and consumers, industry and law enforcement;
- the need for ongoing industry and community – led initiatives.

The closing speech of the final session:

Dear participants,

Concluding our seminar debates, I'm proposing you to accept by consensus the general principles issued at the 2002 EU Forum on Cyber-crime, which can be applied successfully for all the sectors under our today debates - as guidelines for our future activity:

1. The need to respect the rights and freedoms of individuals
2. The need to respect the applicable data protection rules
3. The need to respect competition and public procurements rules
4. The need to respect the legitimate interests of the industries and services involved
5. The need to respect the rights and obligations of independent professions
6. The need to respect the duties and competencies of the interest public authorities, in particular law enforcement and public regulatory and control bodies
7. The need to have a fair share of responsibilities between public authorities and private sector in the implementation of crime prevention schemes
8. The need for partnerships based on voluntary approaches allowing for regular assessment of commitments and of results achieved with a view to permitting adjustments.

Thank you all for your kind cooperation!