COUNCIL OF THE EUROPEAN UNION

Brussels, 29 July 2011

13366/11

LIMITE

COSI 59

NOTE

From:	Presidency
To:	JHA Councellors/COSI Support Group, Standing Committee on operational co-operation on internal security.
Subject:	European Police Chiefs Convention

The Presidency wishes to inform COSI on the outcomes of the European Police Chiefs Convention, which was held at Europol on 29-30 June 2011. High-level discussions and working group meetings were held during the Convention on the future of organised crime and terrorism. As a result, the working groups identified challenges and proposed a number of recommended actions.

The Presidency considers the working groups' conclusions as highly relevant for COSI, especially with regard to the agenda of the forthcoming COSI meeting on 8 September 2011.

COSI delegations are invited to take note of the enclosed introductory letter by Europol's director together with the working groups' conclusions.

EUROPOL

The Hague, 19 July 2011

DIRECTOR

Mr Adam Rapacki
Undersecretary of State

Deputy Minister of Interior and Administration

Chairman of the COSI
By email

Subject: **Conclusions of the European Police Chiefs Convention**

Dear Mr Rapacki,

I would like to take this opportunity to assure you of Europol's full support during The Polish EU Presidency, a challenging period for which I wish you every success. At the same time, I would like to thank you again for attending the first European Police Chiefs Convention and the official opening of Europol's new headquarters between 29 June and 1 July.

It was a great pleasure for me to share with you a historic event for Europol, the official opening of Europol's new headquarters by her Majesty Queen Beatrix of the Netherlands, in the presence of hundreds of senior law enforcement personnel, VIPs and dignitaries, alongside Europol's 700 staff members and other invited guests.

With the opening of Europol's high-tech and dynamic new headquarters, we now have the building to match our ambitions to become a real force in supporting competent authorities in Member States to fight organised crime and terrorism.

The new premises offer great facilities including several state of the art operational rooms and a control centre whose purpose is to coordinate the exchange of criminal intelligence between Member States police forces, EU law enforcement agencies and third countries during major police operations.

The European Police Chiefs Convention, meanwhile, provided Member States and Europol's institutional partners with the opportunity to identify key challenges for EU law enforcement and the development of collaborative responses to future threats in view of preserving the internal security of the EU.

The debates focused on the combating and prevention of serious organised crime and terrorism affecting Europe, with almost 300 Convention delegates participating in high-level discussions and working groups in order to agree on joint directions and guidelines for future policies.

The discussions highlighted potential future organised crime trends such as demographic shifts to drive labour migration leading to increased THB for labour exploitation and facilitated illegal immigration, and geopolitical unrest outside the EU creating large isolated communities vulnerable to the influence of criminal groups. Economic disparity, the lack of synergy between law enforcement and

File no. 2610-218

Eisenhowerlaan 73
2517 KK The Hague
The Netherlands

P.O. Box 908 50
2509 LW The Hague
The Netherlands

Phone: +31(0)70 302 50 00
Fax: +31(0)70 345 58 96
www.europol.europa.eu

legislative bodies and the further development of technology were also seen as future risks.

Delegates called for a more innovative approach to cybercrime and financial crime, with greater emphasis on disruption, prevention, problem solving and systemic collaboration with partners in private sector, NGOs and academia identified as potential responses to these threats. Joint threat and risk assessments by EU security actors, better exploitation of virtual resources and the strengthening of asset recovery and financial investigation capabilities are other topics that need more careful attention in the future.

Considering the future of terrorism, delegates identified several trends, including further fragmentation of some terrorist and extremist groups, the impact of immigration flows on terrorism and extremism, relocation of EU-based terrorist groups in response to law enforcement action, and the increasing importance of the virtual world as a tool, target and weapon for terrorists.

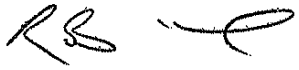
Potential responses to these threats include prevention of radicalisation and de-radicalisation, increased collaboration between law enforcement and intelligence services while maintaining high levels of source protection, flexible public-private partnerships, dialogue with vulnerable communities and an efficient approach in the coordination of the EU's Internal and External Security policies.

Please find enclosed the Working Group Conclusions in relation to Counter Terrorism and Organised Crime, as adopted on 30 June. I am confident that these conclusions as well as the key findings and list of possible responses identified will have a bearing on the discussions at COSI on 8 September and thereafter.

As the Convention and panel discussions were a great success, bringing together leading law enforcement, academic and other practitioners who drafted conclusions which form a solid foundation for future law enforcement policy in Europe, we plan to hold this Convention every year. The next Convention is scheduled for May or June 2012, when I hope to have the pleasure to welcome you once again to Europol's new headquarters.

Thank you for taking the initiative to circulate the Conclusions of the Police Convention to the COSI delegates and I hope that you will find them useful. I look forward to our continued fruitful cooperation.

Yours sincerely,



Rob Wainwright

Director

Annexes:

- The Future of Organised Crime: Challenges and Recommended Actions
- Counter Terrorism Working Group Conclusions

File no. 2610-218

Eisenhowerlaan 73
2517 KK The Hague
The Netherlands

P.O. Box 908 50
2509 LW The Hague
The Netherlands

Phone: +31(0)70 302 50 00
Fax: +31(0)70 345 58 96
www.europol.europa.eu

The Future of Organised Crime

Challenges and Recommended Actions

1. Current Situation

Law enforcement in the EU has made **progress in intelligence coordination and joint investigation** of crimes that are already considered to be priorities. But we have a more limited capacity for monitoring crimes which do not meet this threshold, and for anticipating new trends.

The conservative and **reactive nature of policing** and ever tightening budgets leave agencies insufficiently prepared for new threats. Having enjoyed a monopoly on crime fighting for many years, we remain good at policing what we are comfortable with, but our resistance to change means that we risk developing blind spots for those crimes that we do not routinely investigate.

Cybercrime is a prime example of this. While technology changes on a daily basis, law enforcement often relies on doing what it has always done. Criminals keep one eye on the horizon, but legislation struggles to keep pace and lack of harmonisation sometimes prevents concerted efforts and timely responses from Member States. For all types of criminal activity, asymmetry in legislation and regulatory policy results in displacement, not only between Member States, but between the EU and other parts of the world.

Moreover, the very criminal activities which are identified as being some of the most pressing, lucrative and **rapidly evolving** – such as fraud and cybercrime – are those which until now have received comparatively little concerted law enforcement attention or resources. Where marked progress has been made in stepping up the investigation of cybercrime, this has often been achieved at practitioner level. Given the **financial constraints** under which we all currently operate, we need to consider smarter ways of working.

2. Challenges and Future Risks

Changes in the wider global environment will provide new opportunities for criminal activity. **Demographic shifts** such as an ageing EU population are likely to prove fertile ground for labour migration, raising the possibility of increased trafficking in human beings (THB) for labour exploitation and the facilitation of illegal immigration. In addition, **geopolitical unrest** outside the EU has the potential to create large diaspora communities that are isolated, excluded from mainstream employment, and therefore vulnerable to the influence of criminal groups.

Economic disparity also will continue to bring individuals into greater proximity to organised crime. Poverty, in some cases aggravated by the global economic crisis, has the potential to swell the workforces of criminal groups with not only migrants, but also EU citizens. Projected food crises and other disruptions to supply chains will also fuel markets for counterfeit and stolen goods.

Meanwhile, criminal groups will continue to spot opportunities in **emerging markets** such as alternative energy supply and infrastructure, trade in rare minerals and the disposal of toxic waste, with the risk of monopolisation in markets in which there are large incentives, and which are not subject to sufficient scrutiny or competition from legitimate investors. Equally, illicit activity will continue to have a negative effect on legitimate markets. One example of this is the alleged contribution of metal theft to fluctuating metal prices.

Lack of synergy between law enforcement and **legislative bodies** enables criminals to exploit loopholes and capitalise on demand for illicit commodities. In some cases, controls and regulatory frameworks have themselves proved to be criminogenic. Moreover, the length of time it can take to bring suspects to trial can preclude a timely judicial response, thereby reducing its effectiveness as a deterrent.

The further development of the **Internet and related technologies** will not only put new tools at the disposal of all criminal groups, but will also expose new vulnerabilities in our information society. A future convergence of "entry level" criminal tools and a new generation of technically capable youth raises the possibility of online petty crime. In addition, there is likely to be an increasing overlap between organised crime and terrorist activity on the Internet. Both recent hacktivist attacks on corporations and government websites, and the appearance of tools specifically designed to interfere with the control systems of critical infrastructure (Stuxnet), indicate that this will be a key concern for the future.

The **mass of data** available for investigation, especially pertaining to cybercrime and economic crime, is a clear challenge to established law enforcement capability. It is already no longer possible or efficient to seek to identify and prosecute all suspects for these crimes. At the same time, the volume of this information is expected to expand considerably, as is its role as a commodity from which criminal groups can profit, particularly in light of increased data storage in "the cloud" and a persistently upward trend for use of social media. A more innovative approach is required, with greater emphasis on disruption, prevention and problem solving.

3. Recommended Actions

We must gear up in the fight against organised crime, not only in order to optimise our responses today, but also to prepare ourselves for the challenges of the future. A joined up world requires a crime fighting approach which is equally joined up. A new model of policing is suggested that draws on a network of law enforcement specialists, and emphasises **collaboration with partners in the private sector, NGOs and academia**.

Under this new model, joint threat and risk assessments bringing together a **range of EU security actors** such as Europol, Frontex, SitCen, and ENISA, should provide comprehensive 360 degree analysis of criminal phenomena. In terms of turning strategic findings into operational activity, Project Harmony will do this for crime phenomena that are already subject to law enforcement prioritisation.

We also now need to have a more coordinated approach to traditionally less visible, but no less damaging, phenomena such as fraud and cybercrime. This is not merely a question of financial resources, but of sourcing the **expertise**, and providing the **tools and training** necessary to successfully combat these activities and anticipate their evolution.

Changes in the criminal landscape require changes in law enforcement skill sets. In order to drive forward the fight against organised crime, officers, including Chiefs of Police, must have **greater awareness** of emerging and less visible types of criminal activity, such as cybercrime and economic crime. Investigation tools should be standardised wherever possible, and knowledge of how to exploit virtual resources such as social media should be a **minimum requirement** for the investigation and disruption of organised crime. The judiciary should also be a priority for awareness raising on non-traditional crimes.

More generally, there needs to be clear acknowledgement of the interconnections between global risks and the threat posed by criminal groups, and not merely in the context of assessment. This interconnection demands an **integrated approach to strategic planning** at EU level, with both greater levels of foresight and greater synergies between security planning and economic, energy, social and other frameworks. In particular, those involved in the development of legislative and regulatory frameworks should consult law enforcement with the aim of **crimeproofing** future legislation. There is also consensus amongst experts in a number of different investigative fields that the EU requires **analysis** which goes beyond law enforcement's traditional scope and the envisaged cycle of the SOCTA, to provide Member States and partners with longer range strategic foresight on global issues related to criminal activity.

Public-private partnership is key to our collaborative response, not least because of its global ethos and reach. A first step would be to disseminate the EU's strategic analysis to the private sector to raise awareness, but the primary objective is to minimise vulnerabilities in legitimate markets. Key players in online service provision and the financial sector should be prioritised for outreach for the purposes of information sharing and minimising vulnerabilities in emerging technologies.

In summary, the working group on organised crime advocates a **more creative approach** to combatting criminality that looks beyond traditional law enforcement investigations, prosecutions and surveillance methods, and encompasses a wide range of **administrative and preventative measures**, including serious crime prevention orders already in use in some Member States.

Recognising that the generation of profit is an important motivation for criminal groups, **asset recovery** and financial investigation capabilities must be strengthened, to increase the risk to criminal proceeds. Specific measures such as the establishment of a common EU platform for confiscation, financial reporting orders, and reversal of the burden of proof should also be considered as tools for reducing the rewards of organised crime.

In light of the increasingly blurred distinction between internal and external security, EU law enforcement would benefit from expanding its support and promotion of intelligence-led investigation in developing countries and other areas of the world whose criminal groups impact on Member States. More generally, good practice should be shared on initiatives for **capacity building** in fragile states, with a view to preventing significant infiltration by criminal groups.

Last, but by no means least, we have an unprecedented opportunity to work in partnership with the **citizens of the EU**. The use of Internet services such as social media to generate community intelligence and distribute crime prevention guidance would not only provide reassurance, but would also empower the public to assist law enforcement in the fight against organised crime.

Counter Terrorism
Working Group Conclusions

What can be the future for terrorism?

Further fragmentation of some terrorist and extremist groups

Networks will become looser, terrorists and extremists groups will be able to setup and close more quickly. Technology and the internet, in particular, deliver the capacity for terrorism groups to build a loose network, even from a virtual community, at a very high speed.

An explanation for this could be the lack of leading ideologies in some terrorist forms.

The changing dynamics in our societies, together with technological advances, may encourage isolated, disaffected individuals to turn into violent extremists, to the extreme of becoming 'lone wolf' terrorists.

Terrorism and extremism will shift to more hybrid forms. New types of terrorism such as eco anarchism will come to the scene.

Jihadi terrorism going from a strategic threat to a more tactical threat

The decrease of Al Qaeda's central influence becomes more and more obvious.

The shape of Al Qaeda is not the main issue, the problem is the seeds that were planted a long time ago have grown within European society.

Al Qaeda's current capacity could be measured by any attack carried out. Such a show of strength might ignite passions on both sides of the divide.

The consequences of the Arab spring cannot yet be fully assessed although it presents a huge opportunity for terrorists.

The EU Member States' involvement in conflict zones will continue to impact on terrorist motivations.

Growing immigration flows will impact on terrorism and extremism

The insular nature of some immigration and the lack of integration into societies could lead to an increase in right-wing extremism in the EU. The traditional clashes between right wing and left wing might therefore increase.

Some immigrants from countries with important terrorist activities could offer a bridge between the EU and conflict zones.

Regional shifts

EU-based terrorist groups try to shelter in other countries due to successful law enforcement activities. This will lead to a displacement of terrorist activities in those Member States traditionally less impacted by terrorist activities.

The virtual world will be a tool, a target and a weapon

Society has become more and more dependent upon technology which has the potential for exploitation by terrorists. Almost total dependency on web-based technology may appear as a weakness.

The internet will not only be used as a tool for recruitment, training, planning, as well as being a potential target itself but will also be used as a weapon, for instance on critical infrastructure, and for intelligence gathering.

Terrorists will always study and invest in new technologies in any way possible to facilitate their activities, but the traditional means of attack will remain an easy, cost-effective option for the near future.

Potential economical impact on flows of commercial goods

A non-intentional impact of the cargo bombs was the banning of Yemeni imports into the USA. Similar techniques could have a devastating impact on the flows of global commercial goods.

Symbiosis between organised crime and terrorism

The border between organised crime and terrorism will become more and more blurred. Funding through organised crime activities will become common, and it is still not known whether some terrorist actors will change their motives to those of more personal interest. Organised crime groups might also use terrorist tactics.

What can we do about this?

De-radicalisation and prevention of radicalisation

As radicalisation has been rather intensively studied in past years, the key action needed is the de-radicalisation of radicalised individuals in society. This is the only future we can offer to them. Intensive investment is needed in this area.

Prevention of radicalisation also has to be enhanced.

Tactics and strategies in all dimensions of society must be emphasised. A more integrated approach is needed with all social actors involved: schools, media, police, justice, etc.

Interoperability

Criminal and intelligence databases have to be harmonised and interconnected as soon as possible. Concrete best practices and pragmatic training should then create a real European law enforcement culture.

Flexible private partnerships should also be encouraged as well as dialogue with vulnerable communities.

Police and intelligence services need to reinforce their current collaboration while keeping a high level of source protection.

The use of Interpol's Stolen and Lost Travel Document (SLTD) database must be reinforced by EU and non-EU countries.

Comprehensive strategy for security matters that encompasses all types of threats

The increasing number of strategies and action plans leads to a silo mentality. A clearly defined strategy, identifying the appropriate actors, is essential. The EU security architecture would benefit from integrated approaches to different crime areas including terrorism, border management, serious and organised crime...

Coordinated cost-efficient approach to EU internal and external policy

It is essential that the administrative boundaries that currently exist between key agencies (Europol, SITCEN, Frontex, etc) are eased to facilitate cooperation and information exchange in a more pragmatic way. Is it cost effective that sometimes two organisations analyse the same information?

External policy aspects should also be coordinated, integrating some security dimension.

Changing status of Europol

The borderless dimension of modern crime and terrorism calls for a more ambitious role for Europol. The necessity of two Member States being affected by a criminal act before Europol may legally become involved is redundant in the case of a borderless crime. Europol should be able to engage itself more easily.

In that field, executive powers for Europol may become necessary in some respects.

Obligatory reporting to Europol of all terrorist events in Member States is essential.