



Council of the
European Union

Brussels, 20 October 2015
(OR. en)

13178/15

LIMITE

COSI 129
ENFOPOL 304

NOTE

From:	Europol
To:	Standing Committee on Operational Cooperation on Internal Security
Subject:	Results of the European Police Chiefs Convention, 23 - 24 September 2015

Delegations will find attached the summary of and recommendations resulting from the European Police Chiefs Convention which was held on 23 - 24 September at Europol.



European Police Chiefs Convention 2015

Summary and Recommendations

The Hague, October 2015

EDOC#794993

INTRODUCTION

On 23 and 24 September 2015 in The Hague, Europol co-hosted the fifth European Police Chiefs Convention (EPCC) with the Luxembourg Police¹.

The event was attended by more than 300 senior law enforcement representatives from 45² countries as well as delegates from 10 key international organisations, EU institutions and agencies³.

In preparation for the 2015 EPCC, three working groups were formed, consisting of expert law enforcement personnel, nominated by their national police chiefs, and Europol officials.

Throughout 2015 the working groups examined three terrorism-related subjects in detail so that they could define how international law enforcement cooperation could be better facilitated in the areas of:

- Policing terrorism in our communities
- Policing the terrorist threat online
- Protecting vulnerable communities from the terrorist threat.

On 24 September, delegates discussed the reports of the working groups, resulting in a set of forward-thinking recommendations.

¹ Luxembourg holds Presidency of the Council of the European Union.

² 27 EU Member States plus Albania, Australia, Bosnia and Herzegovina, Brazil, China, Colombia, former Yugoslav Republic of Macedonia, Georgia, Iceland, India, Liechtenstein, Moldova, Norway, Serbia, Switzerland, Turkey, Ukraine and the USA.

³ Council of the European Union, Eurojust, European Commission, European Union Agency for Network and Information Security (ENISA), European Parliament, Frontex, EU Agency for Fundamental Rights (FRA), Interpol, United Nations Office on Drugs and Crime (UNDOC) and the World Customs Organisation (WCO).

SUMMARY

The 2015 European Police Chiefs Convention (EPCC) opened on 23 September, with a working lunch for police chiefs. Delegates were welcomed by Philippe Schrantz, Director General of the Luxembourg Police and Rob Wainwright, Director of Europol.

During lunch, Michael Häuser, Head of Strategic and External Affairs at Europol, presented the key themes that will influence the future Strategy of Europol and invited the police chiefs to share their views on the best ways in which Europol can continue to provide its support to the Member States. Contributions were heard from Austria, Belgium, France, Germany, Italy, Spain and the UK who provided highly supportive remarks and largely concurred with the points presented by Europol.

The police chiefs welcomed initiatives such as the EU Internet Referral Unit and European Cybercrime Centre at Europol, which provide the Member States with new capabilities in a centrally developed manner. In the area of counter terrorism, there was clear consensus that sharing intelligence and working in a cooperative way had always provided the best results. In this context, the police chiefs supported Europol in stepping up its efforts in supporting and strengthening cooperation between the Member States. The police chiefs also signalled the importance of Europol having adequate resources to perform its tasks.

On 24 September, EPCC delegates gathered for the main plenary session, which began with Europol's Director taking the floor to welcome participants. Mr Wainwright emphasised the changes to the organised crime and terrorism landscape since the first EPCC in 2011. Since then, Europol has been increasingly called upon to help coordinate complex and sensitive operations across several jurisdictions. Mr Wainwright noted that Europol was, that same week, coordinating a huge, high profile operation from its headquarters, covering a number of fields of criminal activity and working across many jurisdictions.

Mr Wainwright went on to introduce the main speakers of the plenary session who were to cover the main aspects of the law enforcement community's counter-terrorism efforts in 2015: Frédéric Veaux, Deputy Director of the National Criminal Police (France); Alessandro Pansa, Chief of the Police and Director General of Public Security (Italy); Wil van Gemert, Europol Deputy Director; as well as Alain Bellot, Director General of Customs (Luxembourg); Ignacio Cosidó, Director General of the National Police (Spain); and the keynote speaker, James Comey, Director of the Federal Bureau of Investigation (USA).

The floor was then given to Philippe Schrantz, Director General of the Grand Ducal Police of Luxembourg, which holds the Presidency of the Council of the EU. Mr Schrantz welcomed the participants and emphasised that the Convention met a clear need from law enforcement leaders across Europe. He briefly outlined the current challenges facing Europol and law enforcement cooperation. He continued by saying that terrorism remained a high priority for the Luxembourgish Presidency, especially with regard to the financing of terrorism, radicalisation, and recruitment.

Next, in his keynote address, Mr Comey expressed his strong belief that contemporary law enforcement challenges, especially those related to terrorism and cybercrime, required a multilateral response. Mr Comey shared the FBI's thinking about the threats of terrorism and cybercrime, focusing on the use of social media by terrorists and criminals. He contrasted the *modi operandi* of the old terrorist school of al-Qaeda with the latest ISIL activities. He discussed the way foreign fighters are handled in the USA. Huge resources in the US are being spent on the identification of individuals who are interested in travelling to Syria and Iraq and preventing them from leaving the country. He emphasised that the way to address this new dispersed, rapidly evolving and unpredictable threat is to increase cooperation.

Turning to cybercrime, Mr Comey presented the work in the US of the National Cyber Investigative Joint Taskforce (NCIJTF) incorporating 20 agencies which stay in constant communication to fight cybercrime more effectively. The strategy behind this is that law enforcement agencies must get better at sharing information, including with the private sector. Mr Comey finished his speech by thanking his European partners and Europol for their excellent cooperation.

Two questions were raised following the presentation of Mr Comey. The first question from Ms De Bolle, Chief of the Belgian Police, was on how the US authorities were dealing with the individuals arrested preventively before they leave for conflict zones. Mr Comey informed her that trying to make oneself available to a terrorist organisation was a crime in the US. He admitted that the US has not found an effective way to deradicalise arrested individuals but noted that, in contrast with some European countries, the US does not see a significant problem with radicalisation in prisons. Thus, the preferred solution was to impose lengthy custodial sentences.

The other question was posed by Mr Savona, head of the Transcrime research centre in Milan, Italy. He asked why the ISIL threat was recognised so late by law enforcement authorities. Mr Comey explained that the effectiveness of ISIL's use of social media became clear around spring 2014. The result was seen in the form of a dramatic spike in the number of people radicalising. Mr Comey expressed his opinion that the phenomenon was known from the very beginning but the innovative use of the social media only brought results later.

Police chiefs then debated the outcomes of the working groups, resulting in the sets of recommendations summarised on the following pages.

1 POLICING TERRORISM IN OUR COMMUNITIES

Frédéric Veaux, Deputy Director of the National Criminal Police (France), presented the report of the working group on policing terrorism in our communities⁴. The report explored how terrorism in Europe finds its inspiration in a broad variety of ideologies, including nationalism, separatism, left- and right-wing ideology, and al-Qaeda. The working group decided to focus on the current major terrorist and social threat, known as the foreign fighters (FFs) phenomenon (in relation to the conflict in Syria and Iraq). This phenomenon, based on the attractiveness to young people of the Islamic State and other terrorist groups in the region, is closely linked with the phenomenon of radicalisation, but even more with its violent evolution which later turns into terrorism. All of this has become of great concern for Europe's community of police and security services.

⁴ Led by France with participating experts from Austria, Croatia, Czech Republic, Denmark, Finland, Hungary, Italy, Ireland, Poland, Portugal, Slovenia, Spain, Sweden and Europol.

This report, produced in cooperation with Austria, Croatia, Denmark, Finland, Hungary, Italy, Slovenia, Spain, Sweden and Europol, aimed at reinforcing awareness among EU Member States regarding the terrorist threat relating to foreign fighters. It also aimed to share good practices: based on field experience, EU Member States should communicate about which practical solutions have been successful and to which extent.

In this regard, the report reflected the latest trends among EU Member States. In order to prevent and to better combat radicalisation, some countries had decided to implement specific *hotlines*. The report compared the approaches followed by Austria and by France. The results achieved so far by the hotlines in both countries are very encouraging.

Looking ahead, new terrorist attacks in EU Member States are likely. Both Islamic State and al-Qaeda have the intent and capability to use foreign fighters to carry out terrorist attacks against the EU and the West. Further attacks carried out by unaffiliated lone actors or small groups of radicalised individuals are also likely in EU Member States (MS).

RECOMMENDATIONS

Recommendations made in this document are to be considered in addition to those made in last year's EPCC report.

The EU, based on UNSCR 2178 (2014)⁵, has implemented policies aimed at preventing radicalised young people and young adults from leaving EU MS. This means facing the fact that EU MS are keeping radicalised individuals, or individuals with the potential to be radicalised, on their territory. Once radicalised individuals have left their countries they need to be systematically traced. In this context, common tools developed at EU level should be used and constantly optimised.

⁵ Through Resolution 2178, adopted unanimously on 24 September 2014, the United Nations Security Council condemned violent extremism and decided that Member States shall, consistent with international law, prevent the “recruiting, organizing, transporting or equipping of individuals who travel to a State other than their States of residence or nationality for the purpose of the perpetration, planning of, or participation in terrorist acts.

The working group recommends the following:

1. Enhanced use of the second generation Schengen Information System (SIS II) and Article 36⁶, as well as Article 38, should be continued and encouraged. Using the system to maximum effect, and training first-line responders, should be priorities
2. Specific administrative measures already in place in several EU MS, aimed at preventing radicalised individuals from leaving their countries, such as travel bans, should be continued. For those countries which have not so far implemented such an approach, the sharing of experience with countries that have should be encouraged
3. Making full use of existing Europol tools such as EIS⁷ and SIENA and encouraging EU MS to exchange and share information
4. Enhancing police cooperation on FFs by strengthening the use of the DUMAS Working Group⁸ where several sub-groups driven and co-driven by various EU MS tackle key aspects of the phenomenon⁹
5. Europol's Focal Point Travellers should remain a key tool for addressing the issue of FFs, with the active participation of, and contributions from, all EU MS and associated third parties¹⁰ strongly recommended
6. EU MS should rely on a strong network of police liaison officers/attachés posted in the vicinity of conflict areas
7. A positive outcome from negotiations concerning European passenger name records (PNR) would significantly bolster the EU MS' capabilities to identify and apprehend FFs.

⁶ Regulation (EC) n. 1987/2006 dated 20 December 2006 and ruled by Decision 2007/533/JAI of the Council of the European Union dated 12 June 2007.

⁷ Europol Information System (EIS) and Secure Information Exchange Network Application (SIENA). 'Flagging' of the FFs and potential FFs (travelling to the conflict areas, terrorists hotspots or known training bases), as it has proven to be an effective tool for monitoring FFs. As of now, more than 1200 FFs have been 'flagged' in the EIS.

⁸ The DUMAS Working Group was established in October 2014 and is supported by Europol. It deals exclusively with the issue of foreign fighters.

⁹ Sub-groups include Indicators, Best Practices, Facilitators, and Outreach.

¹⁰ Especially with the Western Balkans.

2 PROTECTING VULNERABLE COMMUNITIES FROM THE TERRORIST THREAT

Alessandro Pansa, Chief of the Police and Director General of Public Security (Italy), presented the report of the working group¹¹ on protecting vulnerable communities from the terrorist threat. The report described the various challenges presented by current terrorist threats to the European Union (EU). Recent incidents in the EU underline the heightened threat. Fighters returning from conflict zones and the emergence of Daesh¹² have a significant impact on the security threat to the EU and elsewhere. Attacks in France, Belgium and Denmark were perpetrated by ‘home-grown terrorists’ who acted alone, or as part of a small cell, with ideological rather than structural connections to recognised terrorist networks, influenced by violent propaganda circulating on the Internet. These incidents could also lead to a breakdown in community cohesion, resulting in greater intolerance, fuelling extremism and violence that, in turn, generates an environment for further radicalisation.

For the purposes of the analysis, vulnerable communities were defined as those directly exposed to violent radicalism. Recent attacks on EU soil have shown that European Jewish communities are directly exposed to this threat, but EU Muslim communities themselves may also be regarded as vulnerable, due to being potential targets for ‘revenge’ attacks, and due to the undesirable radical or extreme elements within the communities that seek to exploit vulnerable individuals to turn them to terrorism. An effective response must be multi-disciplinary, including:

- Comprehensive Security Models;
- Programmes countering violent radicalisation;
- Proactive interaction with vulnerable communities.

¹¹ Led by Italy with participating experts from Austria, Czech Republic, Denmark, Finland, Hungary, Italy, Poland, Spain, Sweden, UK, Europol and Rutgers University.

¹² Daesh is an acronym for the Arabic phrase ‘Dawlat al-Islāmiyya fī al-Irāq wa s-Shām’ (Islamic State in Iraq and Syria (ISIS)), which is mainly used by opponents of ISIS who see ‘Islamic State’ as neither Islamic nor a state.

In order to achieve proactive interaction with vulnerable communities, the report first highlighted the need to ensure that hate acts towards vulnerable communities do not go unreported. There is a need to build an information sharing culture between law enforcement authorities and communities, in order to provide valuable information to law enforcement, useful not only to counter hate-related crimes, but also to identify and manage situations which may lead to terrorist attacks in a timely way.

Contacts should be developed between police forces and leading representatives of the communities, by implementing ad hoc working groups, at a central level, and in-the-field 'counselling centres', which achieve an effective flow of information on events/circumstances symptomatic of, or revealing, a threat. This positive interaction could provide law enforcement with clues or evidence relevant for judicial prosecutions. Data related to transnational aspects should also be forwarded to Europol. Furthermore, any data relevant for assessing the threat, and not only criminal data, should be shared with Europol to take advantage of its analytical capabilities. In a further step, a community policing strand could be created within a technical group of the European Council, to capture and build on some of the existing community based initiatives to counter the rise of hate crime and extremism that leads to violence and terrorism.

John Farmer from Rutgers University (United States) took the floor and applauded Europol for its focus on the issue of vulnerable communities. He mentioned that Rutgers University was engaged in research on securing vulnerable communities both in the US and Europe. The goal was to present an online guide for law enforcement communities to identify best practices, implement them and adapt them to local circumstances. The guide would be released in spring 2016 and could be presented in The Hague.

In response to this suggestion, Mr Wainwright said that with the support of all EU chiefs of police, possibly with leadership from Italy, he would give some consideration to convening a conference on that topic at Europol.

RECOMMENDATIONS

1. Reporting and recording (Better understanding/evaluating the threat)

A first critical point is the issue of under-reporting of hate acts towards vulnerable communities, which has to be seen in relation to the need to build trust and create an environment of interaction between communities and law enforcement.

According to a recent Europol report on anti-semitism¹³, the number of incidents reported during the first half of 2014 roughly doubled compared to the same period in the previous year. By the end of August 2014, a total of 363 incidents had been recorded in the EU, including 20 violent attacks. Perhaps more alarming was the conclusion that these incidents are, more than likely, grossly under-reported.

The risk is that communities perceive an insufficient level of attention from law enforcement towards cases which could be underestimated as minor issues and that, at local level, there could be a lack of adequate sensitivity and, consequently, of a trust environment in which reporting is encouraged.

To be perceived as reliable partners, MS must pay particular attention to the training of first-line officers, who must be effective communicators with a high level of professional competences. The European Agenda on Security of the Commission refers explicitly to the fact that EU funding will increasingly be used to support the specific training of public officials to encourage the monitoring, reporting and recording of hate crimes and hate speech.

Some EU Member States have recognised the need to stimulate communities to report, and authorities to record, the true picture of hate crime in their countries, and they have a number of initiatives in place to facilitate victims' reporting.

¹³ Europol Situation Report: Anti-Semitism in the EU (January – August 2014)

For instance, in 2010 Italy set up the anti-discrimination tool OSCAD¹⁴, which has the purpose of bringing forward under-reported cases, even anonymously, and establishing increasing dialogue and contact with vulnerable communities. In short, OSCAD receives reports of hate acts; starts up targeted interventions at local levels to be carried out by police forces; maintains contacts with associations and institutions, both public and private; prepares training programmes to qualify police operators; puts forward appropriate measures to prevent and fight discrimination.

The UK has created an information and hate crime reporting web portal, known as ‘True Vision’¹⁵. As well as being a general information and awareness-raising portal, the site allows victims to report hate crimes directly to the police, with all hate crime reported being re-directed to a secure police server linking directly with the crime recording systems of the concerned police areas in the UK.

Some other MS (for instance, Finland, Denmark and Spain) also have similar systems offering ‘off-the-shelf’ good practices that can easily be replicated and modified for the needs of States that have yet to develop such models.

These monitoring and analysis frameworks should be rolled out across all MSs, and such tools empowered in order to ensure they are adequate to meet the goal of greatly reducing hate crime unreporting.

2. Information Exchange (Preventing the threat and pursuing hate crimes)

Interaction with communities should go beyond the goal of reducing the number of unreported cases of intolerance and hate crimes.

The significant ‘qualitative leap’ in preventing and reducing the threat is the development of more inclusive and proactive forms of interaction between police forces and vulnerable communities, starting from the premise that effective protection measures should always include continuous and structured listening to potential victims.

There is a need to build an information sharing culture between law enforcement authorities and communities.

¹⁴ Observatory for Security against acts of discrimination (oscad@dcpc.interno.it)

¹⁵ <http://www.report-it.org.uk/home>

When encouraged to meet law enforcement officers at institutional ‘tables’, characterised by a high level of competence and professionalism, representatives of vulnerable communities could share valuable information, useful not only to counter hate-related crimes, but also to identify and manage situations predictive of terrorist attacks in a timely way.

This is why developments should consist of optimising the processes to acquire and transfer - to the national security bodies - the knowledge, the experience and the information owned by vulnerable communities, who are well aware of their situation and are often particularly sensitive to identifying the signs of an upcoming threat.

The contribution of communities, providing details regarding even apparently minor cases, can help to reveal significant risk profiles which, in a first threat assessment based on incomplete information, would not have caught them.

A first goal might be to regularise contacts between police forces and leading representatives of the communities, for instance, by implementing or creating ad hoc working groups at a central level and in-the-field ‘counselling centres’.

These institutional venues can be the ideal context for a usable and effective flow of information on events/circumstances symptomatic or revealing of a threat.

The special dialogue that can be established in this context would positively impact on prevention in all its aspects; at national and EU level.

It would allow police forces to observe the phenomenon from a community viewpoint and hence interpret information and data, including those related to widespread protection and efforts against radicalisation, from a broader perspective, with greater clarity.

Moreover, this positive interaction could provide law enforcement with clues or evidence relevant for judicial prosecutions.

After the necessary probative feedback, law enforcement should provide Europol with data referred to transnational investigations. Furthermore, any data relevant for assessing the threat, and not only criminal data, should also be shared with Europol to take advantage of its analytical capabilities.

3. EU Community Policing Network - Building on successful cooperation models in policing terrorism

In a further step, a community policing (CP) strand could be created within a technical group of the European Council (for instance, EU law enforcement working party - LEWP). This strand could offer an excellent opportunity to capture and build on some of the existing community based initiatives to counter the rise of hate crime and extremism that leads to violence and terrorism. Such a working group could offer EU policing an opportunity to raise awareness of the phenomenon, to scope good practices and to standardise reporting and recording in order to mitigate the spread of hate crimes and identify the stages that lead to violent extremism.

3 POLICING THE TERRORIST THREAT ONLINE

Wil van Gemert, Europol Deputy Director Operations, presented the working group report on policing the terrorist threat online¹⁶. The report assessed terrorist activity on the Internet and the law enforcement response to it. At the outset, it drew attention to the fact that terrorists are increasingly using the Internet to disseminate their propaganda, recruit new members, raise funds and also commit cyber-attacks and hacking activities. Next, it focused on the work of law enforcement agencies in countering the terrorist threat online. In that regard, it distinguished between preventative and investigative police work. The former includes efforts to reduce the availability of terrorist material online, raise public awareness of the terrorist presence on the Internet, and gather enough information to foil terrorist attacks before they materialise. The latter reflects law enforcement's resolve to adapt traditional offline investigative techniques to the needs of the online environment, especially to overcome the obstacles of anonymity and encryption, in order to identify the perpetrators of terrorist criminal offences online.

RECOMMENDATIONS

1. **Adaptation and harmonisation of legislation.** Law enforcement authorities need to work within a legal framework that keeps pace with technology and allows for flexibility. In that sense, legislation must come to terms with the fact that terrorist activity moves from the terrorist organisation to the individual, while at the same time it spreads from the offline to the online world. Changes in law are required to give to law enforcement authorities the ability to detect the early signs of online radicalisation and act to prevent it while prosecuting the radicalisers. In addition, clearer legislation is needed to pursue hate speech, the glorification and justification of, and apology for, online terrorism. Furthermore, legal harmonisation at European level would help to overcome problems in information exchange and coordination of action across borders caused by the deregulation of the Internet and diversification of national legislation.

¹⁶ Led by Europol with participating experts from Austria, Bulgaria, Czech Republic, Denmark, Finland, France, Germany, Hungary, Spain and the United Kingdom.

2. **Strengthening cross-border approach to counter the online terrorist threat.** The global reach and decentralised structure of the Internet fits the transnational nature of terrorism perfectly. As already mentioned, terrorists use Internet platforms on a day-to-day basis to disseminate their propaganda and recruit new members across the globe. Beyond national efforts to counter the online terrorist threat within national borders, **MS acknowledge the need to further enhance cross-border cooperation.** With its central position in the European law enforcement environment, **Europol has an essential role to play** in this issue, both supporting MS's investigations and working on the prevention side. In particular, the creation of the EU IRU, merging skills and capabilities from both Europol's counter-terrorism (O41) and cybercrime (EC3) units, aims amongst others, to upgrade operational and technical support to MS's online counter-terrorism work and reduce - through referrals to ISPs and social media platforms - the availability of online terrorist material. In that context, **MS are encouraged to engage, to the greatest possible extent, with the EU IRU to maximise the effect of cross-border cooperation in the field of online counter-terrorism.**
3. **Advanced training and specialisation.** As terrorists increasingly move to the realm of the online world the presence of specialised law enforcement cadres to monitor terrorist activity, extract useful information, secure evidence, investigate terrorist offences and counter cyber-attacks, becomes a necessity. To that end, personnel's training must focus on the use of new technologies and Internet tools such as social media, applications (apps), dark web fora, etc, which are nowadays commonly used by terrorists. Beyond the training provided by European organisations (e.g. CEPOL, Europol) and national authorities, the exchange of best practice between competent authorities would help European countries to further strengthen their own capabilities in this domain.

4. **Communication and cooperation with the broader law enforcement community.** The dedicated counter-terrorism units should consider drawing on the experience of partner divisions fighting organised crime, drugs trafficking, financial fraud (a.o.) online. The latter, having exposed themselves to online criminal activity, have developed advanced forensic tools to investigate digital crimes and preserve digital evidence. In that regard, a multi-disciplinary approach bringing together the know-how, expertise, and experience of the various law enforcement divisions working on cybercrime would be of added value to online counter-terrorism work. Special thought must be given to the possibility of merging all law enforcement online work in general cybercrime units, pooling resources to deal more effectively with all forms of online criminal activity. In addition, the counter-terrorism units must make the broader law enforcement community aware of how to assess and channel back to them terrorism related information they come across in their online activity. At the same time, all law enforcement personnel must be knowledgeable of the risks of navigating the Internet and the digital footprints they leave with their online activity.
5. **Creating public awareness and supporting communities and vulnerable groups or individuals.** Several law enforcement divisions are deeply involved in raising the public's awareness of different forms of crime such as online fraud, child exploitation, abusive behaviour (bullying), etc. The counter-terrorism units must consider adapting those examples to serve their online counter-terrorism work. Information on terrorist propaganda and radicalisation online can be a useful tool to make Internet users aware of the methods used by terrorists to lure individuals to join them. A constant effort to reach out to the wider society must take place, spreading the message that law enforcement can only increase its efficiency and protect the vulnerable by having the public on its side. Police must work together with the community in identifying individuals vulnerable to the terrorist online message, and also engage with social services and civil society entities to rehabilitate those who have fallen victim to online radicalisation.

6. **Partnership with the private sector.** Law enforcement's capacity to police the online terrorist threat depends significantly on the partnership with the private sector. For police investigators to overcome digital encryption, access remote servers' log files, conduct referrals of terrorist content, etc., the help of the Internet service providers (ISPs), social media companies and other platforms may be of critical importance. Moreover, a strong relationship with the private sector would allow law enforcement to keep track of the latest developments in the virtual world, receive specialised training for its personnel and also get early notifications on changes in the communication patterns of suspected groups of online users. Synergies with the private sector must always be built on mutual trust and a shared interest in upholding the good reputation of all stakeholders.
7. **Engaging with academia.** One cannot overlook the work that has been recently done on counter-terrorism and counter-radicalisation in the academic field. The ability with which researchers elicit information from various sources, build research models, and test theories, has produced valuable results as far as the use of the Internet for terrorist purposes is concerned. The law enforcement community can potentially draw on this work, tapping into the methodology, research and results of the academic world to better understand the evolution of online terrorist activity. At the same time, academic research can benefit from law enforcement feedback on the practical aspects of fighting the online terrorist threat. Lastly, law enforcement and academia can develop common awareness programmes to inform the wider public of the online radicalisation process and terrorist threat.

Mr van Gemert also gave a brief update on the high impact operation Blue Amber being run at Europol at the time of the Convention. Mr van Gemert explained that the operation, when compared to last year's operation Archimedes, was more focused on regions and specific commodities, and the action days were spread throughout the year. Seven Blue Amber action days/weeks had taken place, with impressive results, including 500 arrests and significant seizures. The current action week was focused on drugs, firearms and irregular migration, and involved 29 countries. The preliminary results included 24 arrests, 18 seizures, including the seizure of a major drugs lab, and 110 kg cocaine confiscated – and these were the results of a single day. Mr van Gemert also mentioned that an operation related to the irregular migration crisis was taking place simultaneously at Europol. At the request of the MS, for the preceding 10 days, Europol had established a monitoring centre focusing on the intra-EU migrant flows, complementing situation monitoring at the external EU border delivered by Frontex.

CONCLUSIONS

In the final part of the plenary session, Ignacio Cosidó, Director General of Spanish National Police, talked about **the phenomenon of violent radicalisation and how jihadist terrorism constitutes the most important threat to EU security**. He revealed how the Spanish Police were investing significant resources in designing effective strategies and training programmes to detect, deter and disrupt the efforts of violent extremists to recruit others. Mr Cosidó also spoke about the importance of deradicalisation of often young individuals, and emphasised the crucial issue of information exchange and intelligence gathering. In early 2015, Spain drew up a strategic plan to tackle violent radicalisation, which includes tackling radicalisation in prisons as well. Spain is trying to disrupt radicalisation through specific programmes and by setting up a classification system that enables prison staff and law enforcement officers to identify the early stage of any radicalisation processes. Mr Cosidó continued to emphasise the important role of both bilateral and multilateral cross-border cooperation as essential tools in fighting terrorism. In this context, he called for a greater role for Europol in fighting terrorism.

Dr Jürgen Stock, Secretary General of Interpol, provided information on Interpol's efforts to combat terrorism. He emphasised **Interpol's access to more than 5,000 profiles from 52 different countries**. He also mentioned the joint Interpol-Europol operational investigative global forum on **countering migrant smuggling networks, which Interpol would host in October 2015, with a second meeting to be hosted later by Europol**.

Mr Alain Bellot, Director General of Luxembourg Customs, shared the conclusions of a meeting of heads of customs authorities in Europe held hosted by Europol the previous day. Senior representatives from customs agencies in 22 EU Member States, the World Customs Organisation and Europol discussed the role of customs in fighting serious and organised crime and the existing level of cooperation. Customs directors considered these discussions as the start of a fruitful communication process and expressed their wish to reconvene at regular intervals.

Finally, Mr Liao Jinrong, representing the public security ministry in China, thanked Europol and EU Member States for assistance granted in the areas of fighting cybercrime and terrorism. He expressed the strong commitment of his ministry to the development of a close relationship with Europol and all European countries, and in particular to enhance cooperation on counter terrorism.

Europol Director Rob Wainwright concluded the fifth European Police Chiefs Convention by thanking all the speakers and participants. He summarised the main themes emerging from the discussions around the topic of inter-agency and cross-sector cooperation in counteracting radicalisation and fighting terrorism. Mr Wainwright noted the emphasis that delegates had put on the importance of the systematic sharing of information among agencies at national level and across borders, using Europol channels when appropriate. Slowly but surely, Europol's database on foreign fighters is becoming more complete, and therefore a greater asset for national counter terrorism units. Europol now has over 10 000 suspects in its dedicated database, which is a considerable improvement from what it was just one year ago. He concluded by saying that despite the few brutal terrorist attacks carried out recently, a far greater number of attacks had been disrupted, thanks to the dedication and effective working methods of law enforcement agencies. He believed that it was vital that cross-border cooperation must be part of those methods. Thus, Europol is building up its counter terrorism capabilities to offer services tailored to the needs of the Member States' counter-terrorism units and agencies.

Mr Wainwright then closed the European Police Chiefs Convention 2015.