The Hague, 3 October 2016

CHECK AGAINST DELIVERY

Trends and challenges for law enforcement training and education

Director of Europol, Mr Wainwright,

CEPOL Police Research and Science Conference

Budapest, 6 October 2016

Ladies and Gentlemen,

1. Introduction

- Security was a prominent topic in President Juncker's recent State of the Union speech, as he described need for the EU to defend itself against terrorism and crime. The same day the Commission issued a communication on the EU Security Union - setting out how Europe can enhance its security by improving the exchange of information in the fight against terrorism and by the strengthening of our external borders.
- "The success of what we do in the EU and what you do at Europol in providing security to European citizens is going to decide if the citizens believe in common European solutions to their problems." Those were the words of First Vice President of the Commission Frans Timmermans during his visit to Europol the other day.
- This is no small responsibility. The security challenges today are complex, global and evolving, and have a profound impact on law enforcement across Europe and beyond.
- In order to determine what is required of the police to meet these challenges successfully, we must understand today's threats and be able predict those of tomorrow. And we need to take into account global developments in a variety of areas, which will affect crime and police alike.
- I will structure my intervention along these lines:
    - First talk about today's threats to the security of our societies. That analysis draws on information from up to 40 partners of Europol – EU's Member States and Third Parties, other organisations and

agencies. Europol is – as an operational centre and information hub on serious organised crime and terrorism which receives and analyses information, links the dots and feeds leads back to investigators – well placed to identify threats and emerging trends.

  - Secondly, discuss what this means for national and international police services and their need to learn and develop new skills and tools.
  - Thirdly, discuss Europol's role, with CEPOL, in the continuous learning process of law enforcement in Europe.

2. Threats and drivers

Terrorism

- You will be familiar with the major incidents the last few years: January 2015 Charlie Hebdo, November 2015 Paris again, March 2016 Brussels, July Nice and Ansbach and prior to that London, Madrid and Copenhagen. Add to that a number of foiled attacks.
- The terrorist threat in Europe has escalated. IS and other terrorist groups have increased their level of capacity and network. They want to and are able to strike randomly and at will.
- There is a clear shift towards a broader strategy of IS going global. The terrorist group has developed an external action command trained for special forces-style attacks in an international environment. It is the most significant threat in a decade.
- The threat comes from both lone actors and networked groups. Some attacks, like those in Paris in November last year, were complex, had multiple targets and were directed by the IS. The majority of the attacks in Europe have rather been masterminded by individuals inspired by the group. The attack in Nice was brutal in its simplicity.
- IS terrorist cells operating in Europe are largely domestic or locally based.
- Foreign terrorist fighters may not be a new phenomenon but pose a particular problem. We estimate that 5-6000 European citizens have travelled to Syria and Iraq. Europol has more than 5000 foreign fighters in its database. Recent information indicates that the number of Europeans travelling to conflict areas now is stagnating or even decreasing, but that does not mean that the threat decreases.
- A significant number, approximately 1/3, are returning to Europe and this will continue. Some are then arrested, some rehabilitate, while others are in circulation and constitute a potent threat. Returning foreign fighters may be more lethal than other Jihadist extremists. This is a long term challenge, as are those who stayed at home but may still be plotting attacks.
- Who are they? Mostly young men but the number of women has been increasing, individuals often faced with integration problems or marginalisation, tech savvy using online platforms and social media, radicalising very quickly, a significant portion have been diagnosed with mental problems prior to joining IS, trained by the IS to execute attacks in an emotionally detached way.

- Religious conviction is not necessarily the push factor anymore – that is replaced by peer pressure and role modelling, where suicide bombers see themselves as military heroes rather than religious martyrs.
- IS goes for soft targets – civilians going about their everyday business – rather than symbolic targets. And all countries participating in the anti-IS coalition are regarded by IS as legitimate targets.
- Automatic firearms and home-made explosives have been their preferred choice of weapons, but modi operandi like those in Syria and Iraq, using car bombs for example, may emerge as a method also in Western countries.
- We know of cases where terrorists have used the migration flow to get (back) into the EU, but we have no evidence of this being systematic.
- They use counterfeited passports and other national ID documents, likely obtained from organised crime networks, and get assistance from networks both in the countries of origin and destination. Their communication is of course encrypted and they switch between different platforms to avoid detection. The perpetrators of the Paris attacks, for example, used encryption tools to exchange messages between clandestine cells and the organisers.
- There are links between terrorism and organised crime. More than 800 individuals reported to Europol for terrorism related offences had been reported also in relation to serious and/or organised crime. 6 out of the 10 attackers in Paris and all 5 attackers in Brussels had a criminal background.
- Not to forget: IS is not the only terrorist organisation threatening Western countries. IS does have a greater number of European fighters in its ranks that have combat experience and military training in conflict zones - but Al Quaida is still a factor to consider as the group may try to prove its continued relevance and replicate other attacks.
- We can expect IS and others inspired by IS to attempt more attacks against soft targets in Europe.

Migration

- Migration is the second major challenge for law enforcement. The massive migration flows into Europe over the past years have made the most vulnerable of individuals exposed to criminal exploitation.
- (More than 1 million migrants arrived in 2015, out of which more than half a million came by sea. Some 300.000 have arrived by sea so far this year. The number of persons arriving from Turkey to Greece has dropped significantly, whereas the arrivals to Italy are largely the same as in 2015.)
- An analysis of more than 1500 interviews of migrants showed that more than 90% of the migrants travelling to the EU used facilitation services, mostly offered by criminal groups. Migrant smuggling to and within the EU has become a highly attractive business. Last year alone, criminal networks involved in migrant smuggling had a turnover of between 3 and 6 billion euro.
- Europol's focus and expertise in this area is not on the humanitarian issues or border security but on helping the police tackle organised crime profiting from the migration crisis, and to help identify possible terrorists using the same routes.

- Europol holds intelligence on about 50 000 individuals suspected of being involved in this business – more than 12.000 new suspects have been reported to Europol this year alone.
- In many cases, the criminal groups involved in people smuggling are polycriminal; they are involved in other criminal activities, such as trafficking in human beings (20%), property crime (23%) and drugs trafficking (15%).
- 'Crime-as-a-service' is the business model used by organised crime groups involved in the facilitation of migrant smuggling – they offer fake passports, vessels and other means of transportation, money transfers etc. A large and well organised criminal infrastructure is also involved in the secondary distribution of migrants from the border countries to the rest of the EU.
- Forecast: We expect the migratory pressure on the south eastern route to increase, bottlenecks and informal camps on intra-Schengen borders to emerge, and the use of vessels in poor conditions and private and commercial vans for intra-EU smuggling to increase. We also expect that labour exploitation of migrants in transit and destination countries will continue.

Cybercrime

- Cybercrime is a fast-growing crime area, and a third major challenge to law enforcement today. Cybercrime is borderless and the profits are huge while the risks are relatively low. This is the most enduring, long-term challenge.
- Trends suggest considerable increases in the scope, sophistication, number and types of cyber-attacks, the number of victims and economic damage.
- No country or private company is immune to such cyber threats.
- There are a number of key drivers within the cybercriminal environment, which contribute to the growing proliferation and sophistication of cyber threats.
- The most noteworthy drivers are the increased connectivity and the use of Internet-enabled devices, the borderless nature of the cyber threats, the lack of digital hygiene, the pace of technological innovation, and the Crime-as-a-Service business model, which I mentioned also in the context of people smuggling and terrorism.
- This business model provides anyone, from the entry level cybercriminal to those at the top, with the tools and services they need to carry out cybercrimes, or to amplify the scope and damage of their illicit activities.
- The main cyber trends and threats are:
    - Increased aggressiveness - cybercrime is becoming more aggressive, confrontational and hostile; there is an increased use of extortion (sexual extortion, ransomware, Distributed Denial of Service attacks;
    - Exploitation of existing vulnerabilities - there is a continuous abuse of well-known vulnerabilities due to lack of digital hygiene and a lack of security and a tendency to re-use old tools and techniques;
    - Abuse of current and emerging technologies - increased criminal use of developing and new technologies (Darknet, cryptocurrencies such as Bitcoin, Internet of Things, Artificial Intelligence);

- Sophistication and proliferation of malware - malware remains one of the key threats with significant proliferation of ransomware, information stealers, Remote Access Tools (RATs) and ATM malware;
- Data breaches and growing online fraud - data is a key commodity and enabler for cybercrime. We have witnessed a continuous rise in the number of data breaches. Online fraud is growing steadily as compromised cards details become more readily available online as a result of data breaches and social engineering attacks. We have also seen the first indications of organised crime groups starting to manipulate or compromise payments with contactless cards.
- Live-streaming and self-generated indecent material: Peer-to-peer networks and the growing number of fora on the Darknet continue to facilitate the exchange of child sexual exploitation material, self-generated indecent material and live distant child abuse.

Organised crime groups online – a new world

- Criminal groups today act like multinationals – they diversify and specialise. They are dynamic and quick to exploit changes in the wider environment. They comprise a diverse range of individual criminals, loose networks and organised crime groups, operating across various crime areas.
- Specialised criminals offer their services to other criminals - to migrant, weapons and drugs smugglers, to card fraudsters, money launderers and to terrorists alike.
- The most dynamic criminal markets in Europe today include synthetic drugs and psychoactive substances, counterfeit goods sold mainly online, cybercrime and different forms of environmental crime.
- We expect counterfeit currency, cocaine and heroin crimes to diminish.
- Drivers behind the changing criminal landscape include both socio-economic and technical developments:
    - features of the internet and mobile technology, which are exploited for criminal activities and to prevent detection;
    - the omnipresence and ease of use of devices and services in everyday life, and the increasing operational speed which benefits not only the user but also the perpetrator;
    - the existence of big data – big data and personal data are sought after commodities by criminals groups;
    - the increasing use of e-commerce, which relies on global transportation and logistics, which in turn relies on digital solutions;
    - the increasing mobility of people and ensuing scope for trafficking in human beings, drugs and weapons;
    - nanotechnology and robotics may be in an experimental phase but will open up new markets for organised crime groups;
    - an increasing competition for natural resources may fuel organised crime;
    - the effects of 'deviant globalisation' whereby criminals exploit arbitrary differences in legislation and capability;

  - the general vulnerability of integrated economies to criminal activity; the proliferation of virtual currencies;
  - corruption and the effects of huge organised crime industries;
  - and threats stemming from conflict zones.

3. Impact on law enforcement – the need for training and continuous learning

- The picture today is of a more technology-enabled, entrepreneural, globalised crime and terrorism world. How must law enforcement respond to this?
- The developments behind the changing criminal landscape also offers opportunities for law enforcement, as data and technology can be used to identify, monitor and trace criminals.
- But, the use of the big data in the fight against crime and terrorism requires an exceptionally high level of specialist knowledge and expertise. Law enforcement must ensure that it has the training and resources required to obtain and handle digital evidence, using techniques such as live data forensics.
- The police needs to invest in specialised training to be able to effectively investigate highly technical cyber-attacks.
- As the criminal use of virtual currencies gains momentum, financial investigators will need adequate training in tracing, seizure and investigation of virtual currencies.
- The darknets are often used for cyber-facilitated crime. This is a cross-cutting issue, involving different kinds of crime, and cannot be dealt with only by cybercrime units. Investigators of crime related to drugs, firearms and other illicit commodities, trafficking in human beings and migrant smuggling will also need to investigate in cyberspace – training and tool support must be extended to them too.
- This changes profoundly the methods of investigation in traditional crime areas, like drug trafficking. The value of technology and data is increasing, especially data-sharing. The value for investigators of broader interconnections and communication is growing - connections nationally, internationally and with other sectors. For Europol, the financial institutions and tech sector are of particular importance.
- New investigation skills, a broader set of tools and a good level of understanding of cyber-facilitated and cyber-enabled crime as well as basic knowledge of digital forensics, will be required of all police officers.
- The migration crisis has also entailed new challenges for the police. Many police officers have been confronted with new tasks, requiring new skills, and perhaps being posted to new regions.
- Who is producing the fake life jackets, the fake passports and other IDs, who organises the boats across the Mediterranean and who facilitates the secondary movements within the EU?
- In addition to dealing with these issues in investigations into migrant smuggling and border security, the police have to deal with issues like

vulnerable unaccompanied minors, identifying individuals amongst migrants at risk of being exploited for sex or labour, and security issues in and around asylum centres. They have to deal with politically sensitive public order and criminality issues, while avoiding stigmatizing particular groups.

- And what do you look for when trying to identify returning foreign fighters or facilitators at migration hotspots? Many more police officers will need to acquire these skills.
- Common for all these crime threats is that they are borderless and cyber-facilitated. The speed of the technical evolution demands an adaptive approach to research, training and education – and to funding.
- And it means that front line police need in-depth understanding of the various international law enforcement cooperation tools available as well as inter-cultural communication and language skills. This also entails continuous learning.
    - Academia can play an important role in developing our understanding of all emerging threats mentioned so far. Examples of previous relevant work:
        - Darknet study conducted by TNO in The Netherlands enriched our understanding of online criminal markets;
        - Kings College London contributing to our understanding of the activities and motivations of radicalised extremists who have travelled to conflict zones;
        - Transcrime studies into proceeds of OC and role of 'legitimate' businesses in organised crime;
        - Through Horizon 2020 (EU research funding), several initiatives to improve technical tools for big data analytics.

4. European solutions

- Many countries, in particular smaller countries, may not have police units with this highly specialised expertise, nor the possibility to easily acquire the required skills and tools. They may not be able to keep up with fast and complex technical developments and continuously changing modi operandi of criminal groups and terrorists. Individual countries can simply not do this alone.
- There is also a question of efficiency and funding, of avoiding duplication of work. The solutions are found at European and international level - for operational cooperation and expertise, for information exchange, and for training and education.
- Europol is at the centre of criminal information management in the EU, as a platform with analysts and an operational centre. Europol's innovative technology-enabled platform connects over 600 law enforcement agencies in Europe and partner countries. Europol runs an operational centre on a 24/7 basis and a secure information exchange, supports investigators with cross-checks in our databases on all major crime areas and terrorism, and provides investigators with tailored case analysis.
- Our work is focused around three centres, mirroring the major threats: the European Counter Terrorism Centre, a Centre on serious organised crime

which incorporates the European Centre on Migrant Smuggling, and the European Cybercrime Centre.

- The European Migrant Smuggling Centre (EMSC) has more than 40 experts and analysts providing operational support to the concerned Member States. Europol also monitors smugglers' activities on-line, as they use websites and social media to coordinate and attract migrants.
- As requested by the European Council in March, Europol specialists and Guest Officers seconded by Member States to Europol are deployed to the migration hotspots in Greece – and now also to Italy – to assist the national authorities on the spot with secondary security checks. Europol can thus on-the-spot check for hits of suspected jihadists and migrant smugglers against Europol's systems.
- We can deploy on a longer term Europol Mobile Investigations and Analysis Teams to support Member States in tackling mobile criminals by ensuring on-the-spot smooth and secure information exchange and support with expertise, operational analysis and cross-matching. This also provides for capacity building and the transfer of knowledge - both ways - and helps us identify priority cases. We have deployed these teams to Austria, Hungary, Germany, Spain and Italy.
- Since its launch, the EMSC has received more than 5000 operational contributions and 800 cases have been initiated through our secure communication system. More than 50 high profile cases are currently receiving specialist support from dedicated Europol teams. Europol has also identified 500 vessels of interest and close to 300 cases of document fraud.
- Europol is working closely also with other agencies in this area, including of course Frontex and EUNAVFOR Med. Interpol, which has a Specialist Operational Network against Migrant Smuggling, is another key partner in combatting migrant smuggling. Europol and Interpol are also cooperating closely in fighting cybercrime.

*

- The European cybercrime centre, ECTC, was created at the beginning of this year as a response to the increased international dimension of the problem and the need to have a European perspective. The emergence of links between international crime and terrorism called for information and centralisation of data streams at EU level.
- Fusing classic counter terrorism intelligence with much broader and more mainstream crime data sets has become critical but it challenges the conventional wisdom that counter terrorism is something that can be understood and dealt with exclusively by intelligence agencies.
- For the first time, the EU has a centre that provides the Member States with a set of synchronised tools. It adds a new dimension to the counter terrorism landscape, through the unique set-up with the ECTC and the organised crime and cybercrime centres located in one place, and with expertise in terrorism financing. It will only add value, however, if used by the Member States.
- We have an EU Internet Referral Unit which flags terrorist and violent extremist content online with relevant partners, carries out and supports referrals and provides law enforcement authorities with strategic and operational analysis. The IRU has had almost 10.000 candidates for referral,

and has a success rate of 93 % in having identified extremist content removed (voluntarily) from the internet.

- Europol has also provided substantial support to the French and Belgian authorities following the attacks in Paris and Brussels through a task force (Franternité).

*

- In response to the security threats today, much more needs to be done to fuse relevant information systems at EU level, and to improve the interoperability between systems (SIS, VIS, EURODAC, Europol's systems). Concrete actions to enhance interoperability and information exchange have been taken at EU level, and Europol is actively participating in this work. We are also introducing important changes in the processing of information at Europol as part of the implementation of the new Europol Regulation. These changes will facilitate the work of investigators, as they will improve the possibilities to link information from different systems and different investigations.

Europol and CEPOL

- CEPOL has the leading role in this continuous learning process. Europol's focus is on operational and analytical support to investigators, but we also work closely with CEPOL and contribute to CEPOL's activities.
- Europol participates regularly in various joint activities, webinars, other courses and ad-hoc activities organised by CEPOL. (In 2015 we supported altogether 42 courses and 52 webinars, and this year more than 20 courses and about 30 webinars and a number ad-hoc activities.)
- European Joint Master Programme, launched in December 2014 – Europol contributing to several modules and sponsoring two of its staff to be among the first group of students now following programme.
- CEPOL, Europol (EC3), the Commission, the European Cybercrime Training and Education Group and Eurojust are in the process of establishing a Cybercrime Training Governance Model for law enforcement, which defines the area of responsibility for each partner.
- CEPOL is also involved in the activities of EC3. Together we are developing specific training, ranging from in-depth technical expertise to broader capacity building for police officers, prosecutors and judges notably for cybercrime related casework.
- The demands of confronting these threats are new, highly challenging and unprecedented in many respects.
- It will require a new breed of law enforcement officers, a new mind-set of looking up and out to the world, not down and into the small comfort space of your own district or thematic area of responsibility.
- We need to create a cadre of officers that are adapt to dealing with the high-tech, highly globalised nature of crime today.
- More than anything else, it is a leadership challenge, which has failed so far.
- This cannot be achieved without the right forward-looking and comprehensive training regime.
- This conference, and CEPOL in particular, plays an important role in that.