Trends and challenges for law enforcement training and education

Rob Wainwright
Europol

'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.'

First Vice President of the European Commission,
Frans Timmermans,
during a visit to Europol, September 2016

1. Introduction

Security was a prominent topic in President Juncker's State of the Union speech on 14 September 2016 [1], as he described the need for the EU to defend itself against terrorism and crime. The same day the Commission issued a communication on the further implementation of a 'Security Union' [2], setting out how Europe can enhance its security by improving the exchange of information in the fight against terrorism and by the strengthening of the Union's external borders.

Today's security challenges 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 to predict those of tomorrow, taking into account global developments in a variety of areas.

This paper first describes current threats to the security of our societies and the drivers behind these threats. That analysis draws on information from up to 40 partners of Europol, including EU's Member States, third states and other organisations and agencies. Europol is an operational centre and information hub on serious organised crime and terrorism in Europe, which receives and analyses information, links the dots and feeds leads back to investigators at national level. Consequently, the agency has a unique ability to identify threats and emerging trends. Secondly, the paper discusses what this means for national and international police services and their need to learn and develop new skills and tools. Finally, Europol's and CEPOL's roles in this learning process are discussed.

2. Threats and drivers

Terrorism [3]

Europe has, over the last few years, been the scene of major terrorist attacks resulting in a massive number of casualties. Berlin can now be added to Paris, Brussels, Nice, London, Madrid and Copenhagen as cities that have been targeted by extremists. Add to that a number of failed and foiled attacks, and it is clear that the terrorist threat in Europe has escalated. Islamic State (IS) and other terrorist groups have increased their level of capacity and networking and are able to strike randomly and at will, globally. We have seen terrorist groups acting as external action commandos, trained for special forces-style attacks in an international envi-

[1] State of the Union Address 2016: 'Towards a better Europe — a Europe that protects, empowers and defends', SPEECH/16/3043.

[2] 'Enhancing security in a world of mobility: improved information exchange in the fight against terrorism and stronger external borders', COM(2016) 602 final.

[3] Includes findings in the European Union Terrorism Situation and Trend Report (TE-SAT) 2016, Europol, ISBN 978-92-95200-68-5, and more recent analysis performed by Europol.

ronment. This is the most significant threat to Europe in a decade.

The threat comes from both lone actors and networked groups. IS terrorist cells operating in Europe are largely domestic or locally based. Some attacks, like those in Paris in November 2015, were complex, had multiple targets and were directed by the IS. The majority of the attacks in Europe have been masterminded by individuals inspired by IS rather than conducted by it, however. Lone actor attacks remain a favoured tactic of both IS and al-Qaeda affiliates, who encourage individuals to carry out attacks with whatever means they have at their disposal. The attacks in Nice and Berlin were as brutal as they were simple.

Foreign terrorist fighters pose a particular problem. Europol estimates that 5 000-6 000 European citizens have travelled to Syria and Iraq. Recent information indicates that the number of Europeans travelling to conflict areas is stagnating or even decreasing, but this does not mean that the threat has decreased. A significant number of these foreign terrorist fighters have been returning to Europe, and this is likely to continue. While some individuals are arrested and others rehabilitated, there are also those continuing to constitute a potent threat. This is a long term challenge for law enforcement and other authorities, as are those who did not travel to conflict areas but remained in the EU and may be plotting new attacks.

Who are they? Most of the travelling terrorists are young men, but women inspired or influenced by IS are increasingly taking on an active role. Whether men or women, these are often individuals faced with integration problems or marginalisation and they are radicalising quickly. A significant portion have been diagnosed with mental problems prior to joining IS, and upon arrival they are trained by the IS to execute attacks in an emotionally detached way. They are technology-savvy, using online platforms and social media. Ideology and religious conviction are no longer the only push-factors. Personal circumstances, as well as peer pressure and role modelling, where suicide bombers see themselves as military heroes rather than religious martyrs, are other factors influencing the decision to join terrorist groups.

Automatic firearms and home-made explosives have been the preferred choice of weapons, but modi operandi like those in Syria and Iraq, using car bombs for example, are likely to emerge as a method in Western countries. Regulations on explosives precursors can be circumvented, thus not necessarily preventing terrorists from producing improvised explosive devises.

IS goes for soft targets — civilians going about their everyday business — as well as symbolic targets such as the attack on the Christmas market in Berlin and on religious representatives and police officers. All countries participating in the anti-IS coalition are regarded by IS as legitimate targets and new attacks are to be expected.

There are cases of terrorists having used the migration flow to (re-)enter the EU, but Europol has no evidence of this route being used systematically.

Terrorists use counterfeited passports and national identity documents, probably obtained from organised crime networks, and get assistance from networks both in the countries of origin and destination. Their communication is encrypted and switches 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.

Social media are instrumental in disseminating propaganda material, for the recruitment of volunteers and for raising and moving funds, in order to cover operational expenses related to travel, arms and explosives, false identity documents, vehicles, communication, accommodation and living expenses.

There are links between terrorism and organised crime. More than 800 individuals who were reported to Europol for terrorism related offences had been reported also in relation to serious and/or organised crime. Six of the ten attackers in Paris and all five attackers in Brussels had a criminal background. These connections between criminal and extremist elements could facilitate terrorists getting access to firearms, money and transportation.

IS is not the only terrorist organisation threatening Western countries. IS may have a greater number of European fighters in its ranks that have combat experience and military training in conflict zones, but Al-Qaeda is still a factor to consider as the group may try to prove its continued relevance and replicate other attacks.

EU Member States report that most other forms of terrorism are declining or remaining at low level. Ethno-nationalist and separatist terrorist attacks continue to decrease and left-wing attacks remain rare. On the other hand the right-wing extremist scene has increased its activities in some EU Member States, the key driver being anti-immigration and anti-Islam sentiments.

Migration

Unusually high irregular migration flows pose the second major challenge for law enforcement. More than 1 million migrants arrived to Europe in 2015 [4], out of which approximately half a million came by sea. Approximately 380 000 arrived in 2016 [5]. Migrants from, for example, Syria and Afghanistan continue to use primarily the Eastern Mediterranean and Western Balkan route where they embark on inflatable boats, speedboats or jets-skis and are transported to Greek islands. Migrants from for example Nigeria, Gambia, Senegal, Guinea and the Ivory Coast use mainly the Central Mediterranean Route from the Libyan coast to Italy.

The massive migration flows exposed the most vulnerable of individuals to criminal exploitation. An analysis of more than 1 500 interviews of migrants travelling to the EU showed that more than 90 % had used facilitation services, mostly offered by criminal groups. The annual turnover of criminal networks involved in migrant smuggling is estimated to be between 3 and 6 billion euros. Unaccompanied minors are particularly vulnerable, both during their journeys and in reception centres, representing a specific challenge to law enforcement and other national authorities.

These crime networks are active on various social media platforms, where comprehensive packages of services are offered to prospective migrants. The smuggling networks are getting ever more organised in order to meet the demands for their services.

'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, and other services. 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.

Europol's focus and expertise in this area is on helping the police tackle organised crime groups 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. 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 %). Often they have moved into the facilitation of illegal immigration because it is perceived as particularly lucrative.

Cybercrime

Cybercrime is a fast-growing crime area, and a third major challenge to law enforcement today. Cybercrime is borderless and generates huge profits while the risks are relatively low. While other threats may get more headlines, this is arguably 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.

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 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 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 [6]:

- **Cybercrime-as-a-Service:** a well-established and mature service-based business model that supports the entire cybercrime value chain and drives the digital underground economy. It provides a wide range of commercial and complementary services that facilitate crime online and drives the innovation of tools and methods for committing

[4] Compilation of available data and information, Reporting period 2015, IOM.

[5] Migration Flows to Europe — the Mediterranean Digest, 15 December 2016, IOM.

[6] Internet Organised Crime Threat Assessment (iOCTA).

cybercrimes and cyber-facilitated crimes at unprecedented scale, scope and impact globally.

- **Increased aggressiveness:** Cybercrime is becoming more aggressive, confrontational and hostile, and there is an increased use of extortion, such as sexual extortion, ransomware and Distributed Denial of Service attacks.

- **Exploitation of existing vulnerabilities**: There is a continuous abuse of well-known vulnerabilities and a tendency to re-use old tools and techniques due to a lack of digital hygiene and poor security practices.

- **Abuse of current and emerging technologies:** Criminals increasingly abuse developing and new technologies, such as the Darknet, crypto-currencies and mobile and smart devices.

- **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. There is 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. Europol has also seen the first indications of organised crime groups manipulating or compromising payments with contactless cards. The overall quality and authenticity of phishing campaigns has increased aimed at high level targets.

- **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 operate like multinationals — they diversify and specialise and act globally. They are dynamic and quick to exploit changes in the wider environment, and 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.

Drivers behind the changing criminal landscape include both socioeconomic and technical developments:

- features of the **internet and mobile technology**, which are exploited for criminal activities and to prevent detection;

- the iniquitousness, ever increasing connectivity and **ease of use** of devices and services in everyday life, and the increasing operational speed which benefits not only the legitimate user but also the perpetrator of criminal offences.

- the existence of **big data** and the creation of large 'data pools', comprising large and heterogeneous data repositories including personal data, which are highly sought-after commodities in the underground economy;

- 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, robotics and artificial intelligence** may be still in an early phase but will open up new markets and opportunities 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 socioeconomic effects of huge organised crime industries;
- and threats stemming from **conflict zones**, where instability, corruption, organised crime and violent extremism are often mutually reinforcing.

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

We are confronted with a more technology-enabled, entrepreneurial and globalised crime and terrorism landscape. However, the developments behind the changing criminal landscape also offer opportunities for law enforcement as data and technology can be used to identify, monitor and trace criminals. For instance, the concept of predictive policing ([7]), particularly in the area of crime prevention, could complement the intelligence-led policing approach adopted by many leading law enforcement agencies, including Europol.

The use of big data analytics in the fight against crime and terrorism requires specialist knowledge and expertise as well as dedicated tools, in order to be able to cope with the volume, variety, velocity and veracity of big data.

Law enforcement must also ensure that it has the training and resources required to obtain and handle digital evidence from a variety of different sources, using techniques such as live data forensics and remote access to data stored in the cloud.

Moreover, the police needs to invest in specialised training to be able to investigate highly technical cyber-attacks and other forms of cybercrime effectively. The sophistication and rapid evolution of cybercrimes and the associated criminal modi operandi call for the continuous updating of, and the creation of new, training courses and the proactive sharing of best practices and innovative tactics in order to keep up with the relevant changes and developments.

As the criminal use of virtual currencies such as Bitcoin gains momentum, cybercrime and financial investigators will need adequate training in tracing, seizing and investigating virtual currencies and blockchain analytics.

Darknets such as the TOR network 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 working on drugs, firearms and other illicit commodities, trafficking in human beings and migrant smuggling will also need to be able to investigate in cyberspace — therefore, training and tools must be made available to them too.

This profoundly changes the methods of investigation in traditional crime areas, like drug trafficking. The value of technology and data is increasing, and so is the importance of sharing data, expertise and best practices. The value for investigators of broader interconnections and communication is growing — connections nationally, internationally and with other sectors. For Europol, key partners include financial institutions and the technology sector.

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.

At present, there are large discrepancies across the EU with regard to the technical and financial capabilities of the cyber units and the resources invested in training to investigate such hi-tech crimes. These gaps cause investigative challenges as cybercrime is transnational and requires actions in multiple countries. Some of the main skills gaps which have emerged are in the areas of electronic evidence handling and analysis, online investigations, open source intelligence (OSINT), data mining and big data analytics, alternative payment means analysis, mobile device forensics, and malware analysis. On-going work by the Commission, Europol, CEPOL, the European Cybercrime Training and Education Group (ECTEG) and Eurojust aims to close these gaps by developing a standardised approach to training for law enforcement at EU level.

[7] The concept of predictive policing is the application of mainly quantitative analytical techniques to identify likely targets for intervention and to prevent crime, used by law enforcement to predict future patterns of crime and identify vulnerable areas; it is seen as a method that allows to work more effectively and proactively with limited resources by deriving maximum value from the available data.

The migration crisis has also created new challenges. 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? Many police officers have been confronted with new tasks, requiring new skills, and perhaps entailing being posted to new regions.

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 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. They need to know what to look for when trying to identify returning foreign fighters or people smugglers at migration hotspots.

Common for these threats is that they are borderless and cyber-facilitated. The speed of technical evolution demands an adaptive approach to research, training and education, and to funding. 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 the emerging threats mentioned above. Examples of previous relevant work include:

- A Darknet study conducted by TNO in The Netherlands enriched our understanding of online criminal markets;
- King's College London contributing to our understanding of the activities and motivations of radicalised extremists who have travelled to conflict zones;
- Transcrime studies into the proceeds of organised crime and role of 'legitimate' businesses in organised crime;
- Through Horizon 2020 (EU research funding), several initiatives to improve technical tools for big data analytics.

The expertise held by key private sector actors, which falls outside the remit of law enforcement, is also of critical importance for capacity building and training. Priority should be given to engagement with partners from internet security companies, financial services and communication providers, which have already developed expertise and tools in addressing some of the pressing challenges which obstruct the work of law enforcement investigations in cyberspace.

Furthermore, there is a growing need for cooperation and identifying synergies among the relevant international organisations such as UNODC, Interpol, Council of Europe, NATO, OSCE and others, with a view to aligning and de-conflicting global cyber capacity building and training efforts.

4. European solutions

Many countries, in particular smaller countries, may not have police units with 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 the continuously changing modi operandi of criminal groups and terrorists. Individual countries simply cannot do this alone.

There is also a question of efficiency and funding, of avoiding duplication of work. Solutions can be found at the European and international levels — 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 specialists and as an operational centre. Europol's innovative technology-enabled platform connects over 600 law enforcement agencies and 5 000 officers in Europe and partner countries. Europol runs an operational centre on a 24/7 basis. It provides the platform for 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.

Europol's work is focused around three centres, mirroring the major threats: the European Counter Terrorism Centre, a Centre on serious and 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 relevant national authorities. Europol also monitors smugglers' activities online, as they use websites and social media to coordinate and attract migrants.

As requested by the European Council in March 2016, Europol specialists and Guest Officers seconded by Member States to Europol are deployed to the migration hotspots in Greece — and soon also to Italy — to assist the national authorities on the spot with secondary security checks. Europol can thus perform on-the-spot checks for hits against Europol's systems in order to identify suspected jihadists and migrant smugglers.

Europol can also deploy 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 — in both directions — and helps to identify priority cases. Teams have been deployed to Austria, Hungary, Germany, Spain and Italy.

Since its launch, the EMSC has received more than 5 000 operational contributions and 800 cases have been initiated through Europol's 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 with other agencies in this area, including with 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 Counter-Terrorism Centre (ECTC)** was created at the beginning of 2016 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, including expertise in terrorism financing, and the organised crime and cybercrime centres located in one place.

Europol has 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 already identified almost 10 000 candidates for referral, and has a success rate of 93 % in having identified extremist content removed (voluntarily, by the social media platforms themselves) 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 (Fraternité).

*

The **European Cybercrime Centre (EC3)** was officially launched in January 2013 to provide a joint response to the growing threat posed by cybercrime affecting the EU, with main focus on the hi-tech crimes, transnational payment fraud, and child sexual exploitation.

The added value of EC3's approach in countering cross-border cybercrimes consists of seven key elements:

- providing operational support, coordination, de-confliction, and prioritisation towards focusing the efforts and available resources on the high-value targets and executing impactful joint operational actions;
- using its unique analytical and technical capabilities and the specialised expertise of more than 50 analysts and experts to derive new value from the

data and identify the most dangerous cybercriminal networks and infrastructures, as well as suitable response tactics;

- serving as a criminal information hub and a platform for secure information exchange under a strict data protection framework, where data can be fused towards identifying links among the seemingly unconnected cases and developing actionable cyber intelligence;

- leveraging the networking power to collaborate with law enforcement partners from the EU and beyond, other international agencies such as Eurojust, Frontex, ENISA, and Interpol, as well as working closely with key non-law enforcement partners from private sector and academia;

- developing strategic products on emerging cybercrime threats and trends, as well as cybercrime prevention campaigns to raise awareness about pertinent developments in the field;

- serving as the EU cyber law enforcement's voice worldwide on matters such as Internet Governance, cyber legislation and policies;

- and providing capacity building and training to the EU law enforcement.

Resources permitting, EC3 delivers three 'signature' training courses on an annual basis in its three mandated areas as described above:

- Training on Combating the Sexual Exploitation of Children on the Internet (COSEC): a two-week long course which builds fundamental skills in investigating child sexual exploitation on the internet and helps aligning LE investigative standards, as well as sharing of expertise on innovative tactics and techniques for conducting investigations in this crime area;

- Course on open source IT forensics (OSIT): a two-week training course focused on providing skills for IT forensics analysis using open source tools, especially useful in EU cybercrime units with limited forensic tools at their disposal;

- Payment Card Fraud Forensics (PCF): a week-long training focused on forensic techniques for examining equipment used by cybercriminals and on the retrieval and decoding of stolen payment card data, including practical exercises on forensic examination, payment fraud, criminal modus operandi and evolving crime trends.

In addition, EC3 works closely with the European Cybercrime Training and Education Group), (ECTEG) which supports international activities to harmonise cybercrime training across international borders and provides free training packages to law enforcement on more than 15 topics.

On a regular basis, EC3 experts deliver and provide support to dedicated CEPOL training course, both in-class and online in the form of webinars, in its specialised areas.

EC3 and key partners have also developed the Training Competency Framework (TCF) outlining the required knowledge/competencies and skills for law enforcement and the judiciary in MS, as well as their different training needs.

Moreover, EC3 hosts the FREETOOL project on its secure online platform for cybercrime experts (SPACE). FREETOOL provides a set of digital forensic tools for the cybercrime community, which have been developed by University College Dublin and law enforcement experts. These tools are available for free to law enforcement and are also being used in EC3's training courses. Three of the existing tools will be upgraded and an additional seven will be developed by February 2018.

*

Law enforcement and intelligence services continue to thwart terrorist attacks, and each service holds information on criminal and terrorist suspects. Given the proven connections between organised crime and extremists, a challenge for the near future is ensuring that information between the services concerned is shared and pooled to ensure that connections and leads are identified and investigated, and attacks are prevented.

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. Important changes in the processing of information at

Europol are also being made as part of the implementation of the new Europol Regulation (which becomes applicable in May 2017). 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 the continuous learning process of law enforcement officials. Europol's focus is on operational and analytical support to investigators, but also works closely with CEPOL and contributes to CEPOL's activities.

Europol participates regularly in various joint activities, webinars, other courses and ad-hoc activities organised by CEPOL. In 2015 Europol supported 42 courses and 52 webinars, and in 2016 more than 20 courses, about 30 webinars and a number of ad-hoc activities.

Europol contributes to several modules of the European Joint Master Programme, which was launched by CEPOL in December 2015.

Furthermore, CEPOL, Europol, the Commission, the ECTEG and Eurojust are in the process of establishing a Cybercrime Training Governance Model for law enforcement, which defines the area of responsibility of each partner.

CEPOL is also involved in the activities of EC3. Together CEPOL and Europol 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.

5. Conclusion

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 zone of your own district or thematic area of responsibility.

More than anything else, confronting these new challenges is a leadership challenge. This challenge cannot be addressed successfully, without the right forward-looking and comprehensive training regime.