The Hague, 30 September 2014

EDOC# 737812v3

Europol contribution to the preparation of the Communication on a renewed Internal Security Strategy for the period 2015-2020

By letter from 8 September 2014 from Director-General Matthias Ruete to Director Rob Wainwright, the European Commission has invited Europol to provide a concise contribution to the elements of the consultation on the renewed Internal Security Strategy (ISS) closely linked to the operational mandate and expertise of Europol.

Europol gladly accepts the Commission's invitation and welcomes the opportunity to contribute to the renewed ISS as a corner-stone of the European Union's response to challenges and threats in the area of justice and home affairs.

The Europol contribution contains general introductory remarks related to the renewed ISS and a response to the five questions of the consultation from a law enforcement perspective.

1. General remarks

Europol welcomes the European Council Strategic Guidelines on Freedom, Security and Justice from June 2014 foreseeing a reinforced coordination role for Europol in support of national authorities in the fight against serious and organised crime and terrorism. Europol is committed to mobilise all instruments of law enforcement cooperation in this effort, in particular the improvement of cross-border information exchange, the further development of a comprehensive approach to cyber-security and cybercrime and the prevention of radicalisation and extremism.

With regard to the renewed ISS, the four pillars proposed by the Commission during the recent Council working group meetings covering prevention/protection, information exchange and access to information, international cooperation, innovation and research are all relevant and important for practical operational cooperation.

Also the cross-cutting issues such as strengthening the link between internal and external security, fundamental rights issues, ensuring sufficient resources and funding as well as training are of high significance for effectively combating serious and organised crime, terrorism and cybercrime.

It is important that the ISS provides a clear understanding of the Union's security weaknesses and anticipates future evolutions to better define and adapt policies and strategies. Here, risk and threat analyses such as Europol's Serious and Organised Crime Threat Assessment (SOCTA) or the Internet Organised Crime Threat Assessment (iOCTA) play an important role as a prerequisite for an effective internal security strategy.

The findings of the SOCTA 2013 demonstrate that serious and organised crime is becoming increasingly dynamic and complex, posing a significant threat to the security and the economy of the Union. Europol therefore recommends explicitly emphasizing in the ISS the relevance of effectively fighting serious and organised crime for ensuring a safe and prosperous Europe.

The iOCTA presented in September 2014, calls for much stronger cross-border cooperation, new legislation and legal instruments to detect, attribute and

exchange information, and new partnerships with the private sector to tackle cybercrime.

Europol fully acknowledges the political priority given to migration and border control matters. However, from our perspective, more attention should be paid to the organised crime aspects of irregular migration and, in particular to cross-border criminal networks organising the increasing influx of migrants across the Mediterranean using dangerous means of transport.

From Europol's point of view, the funding allocated to justice and home affairs is still not reflective of the size and scale of the security threats and problems facing the Union and should at least be sufficient to achieve the declared objectives and aims. Given the issue of scarce resources, the ISS should remain focused and succinct and put an emphasis on promoting collaborative options and avoiding duplication.

2. Response to the questions of the consultation

2.1 Which specific challenges need to be tackled by EU action in the coming five years regarding international crime, radicalisation and terrorism, cybercrime and cyberattacks, natural and man-made disasters? What role should the border security have in addressing those challenges?

Challenge #1: Organised Crime Groups are becoming more complex, dynamic and international

Serious and organised crime is an increasingly dynamic and complex phenomenon, and will remain a significant threat to the safety and prosperity of the Union.

A new breed of Organised Crime Groups has been emerging in Europe, capable of operating in multiple countries and criminal sectors - no longer defined by their nationality or specialisation in one area of crime but by an ability to operate on an international basis, with a business-like focus on maximising profit and minimising risk. These new developments are changing the nature of organised crime towards a model based around a networked community of heterogeneous international groups.

In the SOCTA 2013 Europol has identified an estimated 3,600 Organised Crime Groups currently active in the EU, and a lot of these groups are large and mobile networks cooperating with criminal groups all over the world. There is no indication that this trend will be disrupted in the years to come. Indeed the iOCTA 2014 reported a further step in this evolution, in which a service-based criminal industry online, much flatter, more transient and less structured than traditional organised crime is an emerging dominant characteristic of how serious crime is becoming organised. With criminal targets, therefore, becoming less visible and static, and certainly more global in outlook and behaviour, the case for enhanced international law enforcement cooperation has grown.

Challenge #2: The effect of the economic and financial crisis on internal security and the economic impact of serious and organised crime

The deep and sustained financial and economic crisis has made European societies more vulnerable to security threats and has affected the capacity of the Member States' governments to invest in security. Therefore it would be worth considering the impact of the financial and economic crisis on the internal security of the Union in the ISS.

This runs in parallel with the emergence of significant new variations in criminal activity such as commodity counterfeiting, intellectual property rights infringements, tax frauds *(e.g. VAT fraud in the carbon credits market or cigarette smuggling)*, payment card fraud, etc. The black market is expanding and Organised Crime Groups are making billions EUR every year which has serious implications for the Member States' ability to secure an effective economic recovery.

The effects of globalisation on society and business have facilitated the emergence of significant new variations in criminal activity. Criminal networks exploit legislative loopholes, the internet, and conditions associated with the economic crisis to generate illicit profits at low risk.

Challenge #3: Organised Crime Groups facilitating and benefitting from irregular migration

The Strategic Guidelines, the EU crime priorities and the political debate in the Member States underline the need to tackle irregular migration as a matter of priority.

Europol considers that the current debate on how to deal with the influx of migrants by sea should have a greater focus on the disruption of the Organised Crime Groups responsible for facilitating irregular migration. In general, more attention should be paid to the organised crime aspects as an instrument of prevention policies going beyond mere border security issues.

Law enforcement authorities need more information about these Organised Crime Groups. They need to know how they operate in order to identify their criminal masterminds and their trafficking routes. However, the cross-border exchange of information and operational cooperation with regard to irregular migration and in particular with regard to the Organised Crime Groups behind this phenomenon has not been sufficient so far to fully assess the scope of the problem and effectively fight those criminal networks. An enhanced operational coordination and information sharing platform is required in the EU to meet this requirement, a proposal for which Europol has made in 2014 under 'JOT Mare'.

Challenge #4: Terrorism threats, in particular from "foreign fighters"

The threat of terrorism remains strong and clearly has the potential to impact on every part of societal life. For obvious reasons, this is especially so in urban environments. Terrorist modi operandi show increasing use of firearms, emphasis on recruitment and increasing use of Internet and social media.

In the wake of the Syrian conflict, threat of radicalisation is likely to increase exponentially. The so called "foreign fighters" are a serious threat to the Union's security in the years to come, as confirmed by the assessment of the EU Counter-terrorism Coordinator. Here, too, information sharing must improve between Member States and relevant bodies such as Europol. The appetite for this in many Member States is institutionally low, a reality that is somewhat at odds with the nature of the challenge faced. The ISS could encourage a different political mindset.

Challenge #5: Cybercrime threats

Cybercrime is one of the biggest challenges faced by law enforcement today with an exponential growth, rapidly changing modi operandi and being inherently borderless. The high Internet uptake makes the Union vulnerable to cybercrime. This is further compounded by "the internet of things": the more things are connected, the more opportunities for crime there are.

The Internet may facilitate, enable and/or amplify various forms of crime. A number of legitimate features of the Internet are being exploited by cybercriminals such as anonymisation, encryption and virtual currencies, creating challenges for

law enforcement especially with regard to tracing the sources of criminal activity. E-commerce related fraud has increased in line with the growing number of online payments, affecting major industries.

A digital underground criminal industry has established itself with the Darknet being an important platform. Traditional Organised Crime Groups are starting to make use of services offered by the digital underground. Child sex offenders and producers of child sexual abuse content make increasing use of highly anonymous environments such as the TOR Network. Malware is becoming increasingly sophisticated, intelligent, versatile, available, and is affecting a broader range of targets and devices.

The legislative framework has not kept up with technological developments creating vulnerabilities exploited by criminals and triggering new implications for cross-government and private-public cooperation. Differing national legal standards and requirements challenge the success of operations.

Law enforcement practices are struggling to keep up with the pace of change in criminal behaviour and methods. At least 80% of the Internet infrastructure is privately owned. For law enforcement agencies, the main current difficulties are identifying suspects and their whereabouts. Private sector cooperation e.g. of Internet service providers with law enforcement, including provision of user data, is essential in many cases.

2.2 Taking into account the developments in the next five years, which are the actions to be launched at the EU level? How do you see the role of your organisation in supporting those actions?

Action #1: Effectively combating Organised Crime Groups through enhanced cross-border law enforcement cooperation

The renewed ISS should give adequate attention to combating serious and organised crime acknowledging its huge impact on the Union, our societies and the economy. With crime becoming more and more globalised and Organised Crime Groups taking advantage of the opportunities created by greater mobility and the single market, a shift in the Union's strategic response is required towards targeting these dynamic organised crime networks through more effective use of cross-border mechanisms to exchange information and coordinate operational activities.

As law enforcement will and should remain a responsibility of the Member States, the ISS should underline the Union's strong commitment to foster practical cooperation in the fight against organised crime and other forms of serious crime.

A focus on identifying and disrupting the most significant criminal groups should be pursued based on reinforced cross-border analysis. The Policy Cycle for organised and serious international crime, based on Europol's Serious and Organised Crime Threat Assessment (SOCTA) and the EU crime priorities, is a good starting point to improve the quality of decision-making in the fight against serious and organised cross-border crime.

The implementation of the Policy Cycle could be improved by addressing certain shortcomings through providing funding for Multi-Annual Strategic Plans (MASP) and Operational Action Plans (OAP), and stimulating Member States' involvement. The ISF delegation agreement with Europol would be a very important step towards an enhanced operational added value of the European Multidisciplinary Platform against Threats (EMPACT).

The recently implemented Operation Archimedes and hundreds of other major cross-border operations that happen every year in the Union, show that the Policy Cycle and the EMPACT process is beginning to deliver real dividends. Therefore, such action should be further enhanced and supported.

Operation Archimedes has demonstrated that following a horizontal approach, deliberately combining different actions in different crime areas, pays off. After months in the planning, the operation was a carefully coordinated series of attacks on key nodal points and crime sectors that underpin the underground criminal economy prevalent in Europe today. In terms of its scale and impact it ranks as the largest single coordinated assault on organised crime in Europe.

It also shows that close and coordinated cross-border action between police, customs and other law enforcement authorities, supported by the analysis and mobile offices of Europol, and with the involvement of third States, Eurojust, Frontex and Interpol, makes a real difference in the fight against serious and organised crime. Importantly the operation has also provided leads for the conduct of further cross-border investigations.

The ISS should also address the coordination of Member States' action and Union instruments with a view to maximise cross-border cooperation and to ensure that respective tasks are truly complementary, if necessary following a multidisciplinary approach.

Significant efforts are still needed to strengthen cooperation and build trust between the law enforcement authorities of the Member States. As training is one of the most important tools for achieving this objective, the European Law Enforcement Training Scheme (LETS) should be aligned with the ISS.

Action #2: Increasing EU added value to mitigate the Member States' reduced resources and in fighting economic and financial crime

The ISS should identify ways on how to mitigate the risk of a lack of Member States' resources available for internal security due to the financial and economic crisis. Enhanced coordination and cooperation mechanisms at Union level might need to be developed to effectively support the Member States in their efforts to fight serious organised crime.

The ISS should also address the economic impact of serious and organised crime to give a conceptual underpinning to policy proposals in the area of economic and financial crime and actions aimed at securing an effective economic recovery. This would include areas such as tracing and location of criminal proceeds, counterfeiting and infringements of property rights, corruption or the development of Union standards on financial investigations.

Action #3: Disrupting Organised Crime Groups facilitating and benefitting from irregular migration through enhanced exchange of information and coordination

With regard to irregular migration, the Union should pursue preventive measures in third States and at the same time step up the fight against organised crime networks of facilitators. A sustainable strengthening of security through border management requires aligning the tasks of different players such as customs, border guards and police forces at national level and enhancing coordination at Union level.

It is important that the ISS encourages the Member States to share and exchange law-enforcement information and intelligence with each other and relevant EU agencies such as Frontex and Europol, as the basis for any meaningful cross-border cooperation. This is best achieved through building trust, rather than creating new obligations. Without being able to locate and identify the Organised Crime Groups and the individual criminals e.g. by making use of telecommunication data, the police and border guards cannot act, but only react. Apart from that, joint multidisciplinary operations should be developed to strengthen the fight against criminal networks benefitting from irregular migration.

Gathering intelligence certainly requires improvements in the field of travel information, in particular, electronic collection of travel information. Europol therefore welcomes the proposals to establish an Entry/Exit System (EES) and a Register Traveller Programme (RTP). Access by law enforcement agencies, including Europol, to information about place and time of entry to or exit from the Schengen area could help in efforts to prevent and fight crime.

Action #4: Coordinating the fight against terrorism

Counter-terrorism will obviously remain a core competence of Member States requiring concerted action between them and a strong engagement of civil society. Nevertheless the ISS could give some orientation of the supporting EU role in this domain. Key will be effective action to address the issue of foreign fighters. Also in areas such as prevention and countering radicalisation as well as financing of terrorism, which require a more comprehensive and multi-agency response, the EU has an important role to play.

In order to make correct risk assessments and take targeted policy decisions, the Union's intelligence picture on terrorism needs to be improved. The foreign fighters phenomenon has a clear cross-border nature in terms of threat, consequences and vulnerabilities. Therefore a Union-wide common approach is necessary rather than bilateral exchange of intelligence. While the current focus understandably lies on Syria and Al Qaeda/IS related fighters, in the future all forms of terrorism should be tackled by a common approach of the Union.

Europol will continue to provide its annual Terrorism Situation & Trend Report (TE-SAT) and is prepared to assist through providing strategic analysis and operational support via its counter-terrorism Focal Points.

Action #5: Stepping up the fight against cybercrime through legislative initiatives and a strengthened European Cybercrime Centre

More policy coherence in the area of cyber-security is needed. Appropriate, aligned and interoperable legal instruments should be agreed and implemented across the Union to protect against the various threats of cybercrime and Internet facilitated crimes.

Legislation is required to clarify the key principles and values on the Internet including the demarcation between the public and the private domain. In general, legal instruments should explicitly protect the privacy and confidentiality of information in the private domain, as well as privately intended information in the public domain. They should also stipulate the possibilities for online enforcement of the legal framework by competent authorities through surveillance in the public domain and set the conditions and limitations for the use of coercive measures, including intrusion, interception, under-cover operation, seizure, decryption and any other type of data collection and processing.

The definition of minimum standards for security in hardware and software products can help to reduce the harm caused by cybercrime. Also other regulatory measures, such as obliging companies to at least encrypt their repositories of customer data and their payment credentials can lower the risk of data breaches and the abuse of stolen information. Furthermore, clear regulatory guidance is needed in regard to Virtual Currencies.

To ensure that evidence collected and processed in one Member State can be used in other jurisdictions within the Union, it is indispensable to develop and adopt Union standards for digital forensic processing and the establishment of a validation and certification process for digital forensic training and tools.

The private sector has become a key actor of internal security in the EU and there is a need to identify ways of involving it in a more systematic way. The operational necessity for Europol to be able in some cases to directly receive personal data

from private parties has been extensively demonstrated. More broadly, the need for minimum standards on data retention remains highly important for law enforcement and should be regulated in a revised directive.

Clear support, also in terms of funding and human resources, should be provided to the European Cybercrime Centre (EC3) as the focal point of the Union in the fight against this major threat of the 21st century. This should enable the EC3 to pool expertise for supporting the Member States in capacity building and providing operational support to their investigations.

The need for cross-border cooperation in fighting cybercrime calls for working towards a common curriculum for the training of the various actors involved in cybercrime investigations. This should also address the needs of those dealing with the cyber components of traditional crimes. The development of training and tools should also be made available for the benefit of law enforcement authorities of third States from where there is a key treat to online security in the Union.

Much cheaper than suffering losses and investigating and prosecuting criminals is to prevent cybercrime from happening. Joint efforts are required to boost the awareness of citizens and businesses of cyber threats and how to operate online in a secure manner.

The borderless nature of cybercrime calls for more than any other crime type a joint cross-border action. On 1 September 2014 Europol launched the Joint Cybercrime Action Taskforce (J-CAT), piloted for six months, to coordinate international investigations against key cybercrime threats and top targets. J-CAT is composed of Cyber Liaison Officers from MS, third States and EC3 working together at Europol. Similar actions with direct operational impact could make a real difference in the fight against cybercrime. Such actions should be coordinated even stronger through the EMPACT framework, based on the EU-wide threat assessment by the EC3, to ensure well-concerted participation of the Member States and taking full advantage of the central support and coordination function of the EC3.

2.3 Which specific research, technology and innovation initiatives are needed to strengthen the EU's capabilities to address security challenges?

Crucial to enhancing citizens' protection will be using innovation and modern technology in order to enhance the law enforcement authorities' ability to identify criminal networks and their activities.

There is a need for a modern EU intelligence sharing structure and information management architecture. A greater integration and interoperability of systems, possibly around a single central hub at Europol, could help avoid overlapping and duplication of activity, as well as a more efficient alignment of the EU agencies' activities in this area.

For the development of new tools the investments in R&D should be aligned with the actual needs of the law enforcement community and coordinated at Union level to secure the prioritisation, efficiency and relevance of efforts. Union funding should primarily follow the direction provided by the coordinated law enforcement demand.

Europol is enhancing SIENA and has developed a "Universal Message Format" (UMF). There is also a need for a revitalised approach on trans-border exchange of information, building on the European Information Exchange Model (EXIM).

A secure communication system for real-time exchange of operational data would contribute to the effectiveness of all EC3-coordinated operations and would improve a timely response. In addition, an approximation at EU level of "Things devices" in terms of preventing cyber-attacks on Internet and ensuring the integrity of the personal data exchanged through them would be needed.

Law Enforcement faces severe difficulties in attributing crimes to end-users due to the bundling of communication of multiple devices on single IP addresses. The

structural solution for the shortage of IPv4 addresses is the transition to the Internet protocol version 6 (IPv6) convention which extends the number of available IP addresses almost infinitively. In view of the expansion of devices to be connected to the Internet in the near future as part of the Internet of Everything concept, it is most desirable that the transition to IPv6 is fostered, promoted and stimulated as much as possible at policy level.

The contribution of forensic science to different models of policing must be further enhanced. There is in particular a need for research aiming to develop forensic intelligence as an essential component of intelligence-led policing. Efforts should also be pursued to create the European Forensic Science Area.

2.4 What is needed to safeguard rights of European citizens when developing future EU security actions?

Europol is aware of the growing concern in civil society and public opinion about data protection and privacy issues, which needs to be taken into account when developing policies. The renewed ISS will have to ensure that the principle of proportionality is respected, finding a proper balance between ensuring citizens' protection and security, and upholding fundamental rights. For Europol this means maintaining the principle of "purpose limitation" in the implementation of its mandate, as well as the highest levels of data protection.

One of the most important challenges for the Union in this regard will be to reach a lasting political consensus on the balance between security and freedom in the context of serious criminality operating online and across borders to a much greater extent than ever before. The new ISS has also to take into account the growing e-dimension of society.

Also the discussion about data retention should be seen in this light. Although the ECJ found in April 2014 that the "electronic communications Directive" was invalid, the Court did also find that the objective of this Directive, namely retaining telecommunication traffic data in order to protect public security, is a legitimate objective.

It is also important that any general data protection regime takes into account the specificities of the law enforcement area and does not create unnecessary administrative burdens on already stretched national police forces in terms of extensive information obligations, or that it creates serious limitations to lawful international police information exchange, especially in view of the threats coming from globalised organised crime and terrorism.

Ultimately, we have to avoid a situation where current cooperative relationships between the Member States' law enforcement forces are negatively affected or Member States become reluctant to share information at all.

2.5 How can the EU's foreign policy improve the security within the EU?

Many of the criminal threats the EU is facing, and several of the EMPACT priority areas, have a significant external dimension as an increasing number of Organised Crime Groups operate on an international level. Combating these threats requires strengthened cooperation within the Union and with external partners. Hence, the need for more coherent use of foreign policy instruments for internal security purposes is indisputable. This process would be greatly facilitated by more frequent, better-structured and formalised relations between Europol and the European External Action Service (EEAS). At the decision-making level, enhanced coordination and cooperation of COSI and PSC, as well as other relevant bodies, would be desirable. At the very least, however, the foreign policy agenda of the EU should carry a much higher interest in security issues than has evidently been the case thus far.

Better information exchange is the first step towards a more coherent security policy as EU delegations, missions and operations have access to information that could be of value for Europol. This ranges from open sources to operational criminal intelligence/personal data in case of CSDP missions with executive functions.

Foreign policy could be instrumental in facilitating the exchange of information between Europol and third States, as some of the exchange can be based on agreements concluded by the Union pursuant to Article 218 of the Treaty on the Functioning of the European Union.

Security issues should become a more prominent element of the dialogue with external partners. This could also be guided by assessments made by Europol and other JHA agencies. Foreign policy, in particular accession and visa liberalisation talks, could be linked to security-related conditions and requirements. They may include, depending on the specific threats stemming from the country in question, closer cooperation with certain EU agencies such as Europol. The Union could also indicate crime fields which need to be prioritised by the partner.

Finally, foreign policy could be instrumental in coordinating EU-supported security initiatives in third States and regions. This would also include prevention initiatives that overlap with activities already undertaken at Union level and streamlining the existing ones, so that they properly mirror the Union's priorities in the field of internal security.
