EUROPOL

EXPLORING TOMORROW'S ORGANISED CRIME

EUROPOL
EUROPEAN LAW ENFORCEMENT AGENCY

Table of Contents

Exploring tomorrow's organised crime

SOCTA Academic Advisory Group

FOREWORD
BY THE DIRECTOR

I am pleased to present Europol's view on the future of serious and organised crime in the European Union (EU). This report, a first of this kind for Europol, is the outcome of our engagement with experts in the private and public sectors and academia as well as our many partners in the European law enforcement community.

Law enforcement is often criticised for being reactive rather than proactive. A reactive approach to criminal offences committed lies in the nature of police work — in solving criminal cases, supporting victims and working within our judicial systems to create justice. However, we can also be more proactive in fighting crime, particularly organised crime, in anticipating the development of new modi operandi, shifts in criminal markets and changes in organised crime structures. Looking ahead will enable us to better allocate resources, plan operational activities and engage with policy- and law-makers to prevent certain types of crimes from emerging.

This document considers the future of serious and organised crime in the EU and while we do not claim to make definitive predictions, we identify a series of key driving factors that will impact on the serious and organised crime landscape in Europe.

The EU's first full multi-annual policy cycle on serious and organised crime enters its third year in 2015. The policy cycle represents Europe's joint effort in fighting serious and organised crime and aims to coordinate the activities of many stakeholders at EU-level. With the first successful operational actions of this cycle already accomplished, this is an ideal time to look ahead and identify the key trends and developments that will shape our wider environment, law enforcement and serious and organised crime.

Serious and organised crime will pose new threats to the Member States of the EU. Organised crime groups will find ways to exploit evolving technologies, changes in the economy and society. New forms of payment such as virtual currencies will change how criminal actors transfer and launder illicit proceeds of crime. New modes of transportation will provide OCGs with greater mobility and new ways to traffic illicit goods into, from and via the EU. Economic disparity and declining prosperity in EU Member States has the potential to create a climate rife for exploitation by OCGs and creating large pools of potential recruits for organised crime. The increasing scarcity of and competition for natural resources will open new fields of exploitation for OCGs. The make-up of European societies is undergoing major demographic changes opening up new opportunities for OCGs to exploit a larger group of elderly people or provide illicit services to them. These and many other factors are set to impact on the serious and organised crime landscape. Organised crime is dynamic and adaptable and law enforcement authorities across the EU are challenged to keep pace with the changing nature of this substantial and significant threat.

However, just as criminals learn to exploit new technologies and invent new modi operandi, law enforcement authorities also make use of technological innovation and develop new investigative measures to counter the threat of organised crime. In this report, leading police officers from various EU Member States, third partners and international organisations outline how they evaluate the challenges and opportunities facing law enforcement over the next decade. Law enforcement authorities are becoming more effective and better at countering the various criminal threats emerging from serious and organised crime. Law enforcement authorities will continue to innovate to serve and protect their communities across Europe.

We hope to be able to make a contribution to their work with this report by outlining potential developments and emerging threats across the serious and organised crime landscape.

> *Organised crime is dynamic and adaptable and law enforcement authorities across the EU are challenged to keep pace with the changing nature of this substantial and significant threat.*

Rob Wainwright
Director of Europol

INTRODUCTION

This report outlines key driving factors for the evolution of serious and organised crime in the EU. The document describes these key drivers, their impact on serious and organised crime and the potential impact on individual crime areas and organised crime groups (OCGs). It does not claim to make definitive predictions or provide a complete picture of crime in the future, but rather aims to outline plausible developments and to encourage law enforcement authorities to consider and explore the potential evolution of serious and organised crime.

The report opens with a discussion of Europe's changing criminal landscape and the key drivers that will impact on serious and organised crime over the next decade. The key driving factors presented in this document were inspired by the Serious and Organised Crime Futures Forum held at Europol in March 2014. The Forum brought together experts from government, the private sector, think tanks and international organisations as well as a large number of law enforcement experts from various Member States and third states associated with Europol. In a two-step process, all participants first identified key driving factors in the environment. Law enforcement professionals then engaged in discussions to outline the potential impact of these factors on serious and organised crime. The report focuses on those key drivers with the most profound impact on serious and organised crime in the future. These fall within two categories, technology and socio-economic developments, and are each discussed by focussing on their general impact and their impact on serious and organised crime specifically.

In addition to exploring potential developments in serious and organised crime, the report also provides a view on the future of law enforcement and how law enforcement authorities across the EU and on a global level may seek to counter and contain organised crime activities over the next decade.

Europol also benefited from the advice of the Academic Advisory Group for the Serious and Organised Crime Threat Assessment (SOCTA), which reviewed the document and provided extensive feedback on the findings of the report.

© Shutterstock

Serious and Organised Crime Futures Forum
12 & 13 March 2014

KEY TRENDS

FOR THE FUTURE OF SERIOUS AND ORGANISED CRIME

A decline of traditional hierarchical criminal groups and networks will be accompanied by the expansion of **a virtual criminal underground made up of individual criminal entrepreneurs**, which come together on a project-basis and lend their knowledge, experience and expertise as part of a crime-as-a-service business model. This criminal market dynamic is already realised in the realm of cybercrime, but in the future will also extend to the domain of 'traditional' organised crime and govern crime areas such as drugs trafficking, the facilitation of illegal immigration or the counterfeiting of goods. In this **fragmented and global criminal market** criminal actors will engage in **'co-opetition'**, which sees competing actors interact or cooperate in the ad hoc pursuit of criminal opportunities.

Less reliant on established criminal groups and hierarchies which can be more easily targeted by law enforcement, criminals will simultaneously diversify their activities and specialise in the expertise they offer. Criminal actors, both groups and increasingly individual criminal entrepreneurs, will adopt the **crime-as-a-service business model**, which is facilitated by social networking online with its ability to provide a relatively secure environment to easily and anonymously communicate. In the pursuit of new clients, organised crime will invariably seek to **change the commodities** they trade shifting from traditional goods to new commodities.

Almost all types of organised crime activities will rely on **digital infrastructures**. The trade in illicit goods and the exchange of money will take place in the virtual realm requiring little face-to-face interaction between trading partners and reducing risks of discovery and interception. Virtual currencies will allow organised criminals to anonymously exchange and use financial resources on an unprecedented scale without the need for complex and cost-intensive money laundering schemes. Some actors will provide highly specialised services catering to a relatively small group of clients. These services may include the **infiltration** of control systems or the physical infiltration of companies using sophisticated identity fraud scams with information gathered from online intrusion and reconnaissance.

Serious and organised crime will continue to target vulnerable people for exploitation and seek to open up new pools of potential clients for illicit goods and services. However, patterns of criminal activities and **the groups of people targeted as victims and clients will change** over the next decade. The elderly, a growing segment of society, will emerge as a main target and client group for organised crime. Criminal actors will seek to exploit elderly people and offer new services tailored to them. Shifts in routes and movement patterns may involve the increasing targeting of EU citizens for their trafficking to emerging markets for sexual or labour exploitation. **Legal business structures will be targeted on an unprecedented scale,** even more than was previously the case, both as victims of crime and as targets of infiltration to be used as vehicles for other criminal activities.

The future of serious and organised crime:

• **A virtual and global criminal underground** made up of individual criminal entrepreneurs

• Using a **crime-as-a-service business model** and trading in diversified commodities

• Relying on **digital infrastructures, virtual currencies and infiltration**

• Targeting changing pools of victims and clients such as **the elderly or legal business structures**.

Transportation and logistics

Nanotechnologies and robotics

Data as a commodity

E-waste

Economic disparity in the EU

Increase of competition for natural resources

Proliferation of virtual currencies

Demographic change in the EU

Key drivers for change

Innovation in **transportation** and logistics will enable OCGs to increasingly commit crime anonymously over the internet, anywhere and anytime without being physically present.

Nanotechnology and **robotics** will open up new markets for organised crime and deliver new tools for sophisticated criminal schemes.

The increasing exploitation of **Big Data** and personal data will enable OCGs to carry out complex and sophisticated identity frauds on previously unprecedented levels.

E-waste is emerging as a key illicit commodity for OCGs operating in Europe.

Economic disparity across Europe is making organised crime more socially acceptable as OCGs will increasingly infiltrate economically weakened communities to portray themselves as providers of work and services.

OCGs will increasingly attempt to infiltrate industries depending on **natural resources** to act as brokers or agents in the trade with these resources.

Virtual currencies increasingly enable individuals to act as freelance criminal entrepreneurs operating on a **crime-as-a-service** business model without the need for a sophisticated criminal infrastructure to receive and launder money.

OCGs will increasingly target but also provide illicit services and goods to a growing population of elderly people exploiting **new markets and opportunities**.

9

1

TOWARDS A NEW DEFINITION OF ORGANISED CRIME?

Europe's changing criminal landscape

Organised crime continues to challenge the law enforcement authorities charged with protecting the citizens of the European Union. OCGs are as varied as the markets they service and the activities they engage in. In many cases, OCGs reflect the societies, cultures and value systems they originate from. As societies across Europe become more interconnected and international in outlook, organised crime is now also more connected and internationally active than ever before. The group structures that dominate fictional representations of organised crime are disintegrating and will increasingly give way to an organised crime landscape dominated by loose networks made up of individual criminal entrepreneurs who interact and conduct their business in a shared, and often digital, criminal underworld. This introductory chapter sets out a picture of future developments in the organised crime landscape in the EU, providing a context to the key factors driving change discussed in later chapters.

Economic and social change prompted by migration, more diverse and multicultural societies, demographic change as well as technological innovation impact on the nature of OCGs and individual criminals. Unprecedented socio-economic transformations across Europe over the past 70 years have called into question traditional value systems and fundamentally changed social structures. This is particularly apparent in the decline of collectivist attitudes among Europeans and the emergence of greater and more pronounced individualism.

These changing norms and expectations also impact on organised crime. Since the year 2000, the United Nations Convention against Transnational Organized Crime has provided an internationally shared definition of an organised criminal group as a group of three or more persons existing over a period of time acting in concert with the aim of committing crimes for financial or material benefit. This definition continues to reflect law enforcement authorities' conceptualisation of organised crime across the world, but does not adequately describe the complex and flexible nature of modern organised crime networks.

OCGs operate in a criminal economy dictated by the laws of supply and demand and are favoured by social tolerance for certain types of crime such as the trade in counterfeit goods and specific frauds against public authorities or large companies. These factors will continue to shape the organised crime landscape. The boundaries between legal and illegal activities are becoming more blurred and defining organised crime is increasingly difficult. Individual criminals and criminal groups are flexible and quickly adapt to exploit new victims, to evade countermeasures or identify new criminal opportunities. Political and legislative changes such as the introduction of new free trade agreements and a further enlargement of the EU are certain to impact on the activities of criminal groups in the EU. However, the accession of additional Member States to the EU also provides law enforcement authorities with new opportunities for cooperation and the exchange of knowledge.

A service-oriented criminal underworld

The anticipated development of criminal networks engaged in 'traditional' organised crime activities, such as drug trafficking or the facilitation of illegal immigration, mirrors the evolution of criminal actors and criminal networks involved in cybercrime. Cybercriminals already operate as part of an online community which is complex and highly dynamic yet fragmented. Europol's iOCTA 2014 identifies crime-as-a-service as a key feature of the digital underground economy.

The organised crime landscape in Europe will be increasingly dominated by loose, undefined and flexible networks made up of individual criminal entrepreneurs. Criminals work on a freelance basis and are no longer part of a bigger network or group. Coming together as service providers to support project-based criminal endeavours, they inhabit a broader criminal underworld, which is already heavily facilitated by the internet.

Increasingly, these criminal actors will come together on online platforms to plan specific criminal activities or coordinate their roles in existing criminal projects. So far, this has been true for activities in the realm of cybercrime, but the emergence of online marketplaces where crime-as-a-service offerings are exchanged will increasingly extend to more traditional forms of criminality.

An anonymous internet-facilitated marketplace for criminal services also carries the risk of enabling a convergence between organised crime and terrorism. Criminal entrepreneurs delivering services not based on allegiance to specific OCGs but exclusively driven by profit- incentive will have fewer inhibitions about collaborating with terrorist groups. Radicalisation and the return of foreign fighters to the EU are also likely to impact on the nature of organised crime. Those returning or radicalised for extremist causes will often inhabit the same broader criminal underworld that sustains organised criminal networks.

Organisational crime

In some cases, criminal behaviour is socially accepted, especially when it is intended to circumvent legal provisions perceived as 'over-regulation' and when it serves to maximise profits gained from otherwise legal activities.

Traditionally, corporate crime was not pursued by law enforcement authorities as actively as other forms of criminal activity. Some forms of corporate criminality were accepted as a cost of doing business and a minor concern so long as companies provided employment and benefited the overall economy. Organisational or corporate crime was overlooked and under-investigated. However, a series of scandals involving corporate crimes publicised in the press in the early 2000s highlighted the impact and cost of these activities. Criminal activities carried out by corporations are likely to occur at least as frequently as other forms of crime. Targeting organisational crime remains difficult: companies and administrations do not want bad publicity and often these crimes remain hidden from the public and law enforcement. Except where there are whistleblowers, many cases of corporate crime only come to light once a larger group of victims is affected. The

economic crisis has revealed serious and in some cases criminal misconduct carried out by banks and businesses to the financial detriment of millions of victims. While this substantial economic damage was not usually intentional, the wilful neglect of due-diligence and ignoring of financial regulations in some cases

> *The organised crime landscape in Europe will be increasingly dominated by loose, undefined and flexible networks made up of individual criminal entrepreneurs. Criminals work on a freelance basis and are no longer part of a bigger network or group.*

amounted to criminal activities, as reflected by fines imposed as a result of several court cases in the United States and Europe.

Investigating organisational crime remains difficult. Currently, there is much dispute about the scale and precise nature of organisational crime, requiring additional research and targeted investigations. Debates on how to counter corporate crime from a legal and policy perspective remain difficult and are often fraught with the conflicting interests of balancing business needs and regulations. In many jurisdictions, the role of law enforcement in investigating corporate crime is not clearly established.

The globalisation of business through the exponential rise in foreign direct investment and the emergence of truly international corporations make investigating corporate crime an even more challenging task. Corporations already choose their place of incorporation to minimise taxes and some corporations may choose 'light touch regulation' countries where lax regulations and social acceptance of some criminal behaviours benefit business models that rely on some criminal activities to facilitate them.

Exploiting legislation

Legislation has been and will continue to be a key factor determining the nature and extent of organised criminal activity across Europe.

Laws governing immigration, the setup of social benefit systems, taxes, trade, competition, environmental protection and many more areas all shape what OCGs do and how they conduct their criminal business. While the EU has made progress in harmonising some areas of legislation with an impact on serious and organised crime across Member States, many areas of law still feature greatly varying provisions between different Member States. These legislative differences and a proliferation of legislation across the EU create loopholes and opportunities for organised crime. OCGs are already adept at using specialist knowledge and expertise to maintain sophisticated and complex criminal enterprises engaging in crimes such as VAT fraud or the illegal trade in waste. In the future, OCGs will be even more committed to investing in legal expertise exploiting legal loopholes of an expanding body of law across the various jurisdictions of the EU. The harmonisation of criminal justice legislation would also make it increasingly difficult for criminals to escape prosecution by fleeing individual jurisdictions. Some convergence is already taking place at EU-level.

However, a proliferation of differing legislation across EU Member States will make it easier for criminals to exploit loopholes. Entities committing organisational crime already have access to the best legal expertise available on the commercial market and will present an increasing challenge to law enforcement.

2

KEY DRIVERS FOR AND THEIR IMPACT ON ORGANISED CRIME

Organised crime will undergo profound and significant changes over the next decade in response to the availability of new technologies, changes in the environment such as economic challenges or developments in society and in response to law enforcement actions. Organised crime will undergo these changes whether or not experts agree on a new definition of organised crime and it is imperative for law enforcement to seriously consider the factors and driving forces that will shape serious and organised crime over the coming years.

© Shutterstock

CHANGE
SERIOUS AND

- Transportation and logistics
- Data as a commodity
- Nanotechnology and robotics
- E-waste
- Economic disparity within the EU
- Increased competition for natural resources
- The proliferation of virtual currencies
- Demographic change in the EU

15

Innovation in transportation and logistics will enable OCGs to increasingly commit crime anonymously over the internet, anywhere and anytime without being physically present.

Revolutionary road

The EU benefits from well-developed transportation and logistics infrastructures, which move people and goods across Member States. The transportation and logistics sector is of crucial importance to Member States' economies and provides employment for millions of people in the EU. Private households in the EU spend more than 10% of their total annual expenditure on travel and commuting. Large volumes of freight are transported throughout the EU.

In the future, transportation and logistics in the EU will need to service the continuously growing demand for increased mobility of people and goods, while reducing the environmental impact of the technologies used. [1] In order to ensure customer satisfaction, the EU's transportation and logistics sector will need to provide energy- and cost-efficient means of moving goods and people. Environmental concerns and increasing pressure on resources will make the principle of a sharing economy increasingly popular. This economic model favours alternative modes of transportation such as new forms of mass public transit and on-demand ride services enabled through online applications in addition to established models like car- and bike-sharing. Advances in technology and the increasing exchange of data will facilitate these developments. Fuel may become prohibitively expensive to individual commuters and this may encourage car-sharing enabled by online applications.

Innovation and development in transportation and logistics require significant capital investments: the financing of new projects and the maintenance of existing infrastructures will be a key issue in this sector. Project funding will increasingly rely on public-private cooperation. In logistics, crowd-sourcing schemes might be used to make supply chains more cost-effective. For instance, citizens living and travelling in urban areas on a daily basis may coordinate the delivery of packages amongst themselves. Collaboration between competitors, so-called 'co-opetition', will make transportation and logistics more cost-efficient and sustainable. Global trade will continue to increase each year and will require the creation of new modes and routes of transportation resulting in the emergence or further development of a number of key global infrastructure hubs. China and Brazil are likely to continue their development as key markets for transportation and logistics. Central Asia is likely to emerge as a key transit region. The melting of the arctic ice will enable the use of shipping routes in the Arctic Ocean that were previously inaccessible. New routes connecting parts of Asia, North America and Europe will result in a diversification of maritime transportation options providing for faster and cheaper transit of goods.

E-commerce will rely heavily on an efficient global transportation and logistics sector to sustain its unprecedented growth and to service customers in all parts of the world. Courier, express and parcel services will become increasingly important and sophisticated requiring more regional warehouses closer to delivery markets. Securing these warehouses and supply chains will become increasingly difficult and different delivery models for this security will emerge, involving both the private and the public sector.

Much future mobility will rely on digital solutions. Many of these will use Big Data analysis often involving real-time open data.

©istock

The integration of transport infrastructure develop-ment with digital infrastructure development will be essential in order to ensure efficient and effective transportation networks. Innovations in information technology, automation and robotics will bring new types of vehicles onto the market. Unmanned Automatic Vehicles such as self-driving cars and Unmanned Aerial or Maritime Vehicles will become widely used. Both Google and Nissan have already an-nounced the development of self-driving cars, which promise to provide more flexibility for transportation businesses and more independ-ence for individual travellers.
'Personal fabrication' using 3D printers will change tomorrow's logistics. In many cases, the production of goods will take place closer to the point of delivery, often in so-called "fab shops" or at home. However, raw materials for 3D printing will still need to be delivered to the place of fabrication.

Travel into the future of crime

The transportation and logistics sector will continue to grow significantly. Some of the anticipated changes in this broad and vital sector will be revolutionary. OCGs will find new and innovative ways to exploit changing modes of transport, new routes and technologies. New technologies will enable the fast and often undetectable movement of large quantities of illicit commodities. As transportation and logistics infrastructures rely more and more on online systems and automated remote manage-ment, OCGs will increasingly rely on intrusion into these systems to manipulate transport routes, infiltrate supply chains and gather valu-able and sensitive data.

These far-reaching changes in transportation and logistics will have a significant impact on serious and organised crime. OCGs will seek out opportunities to attack or infiltrate transpor-tation and logistics infrastructures and hubs to

facilitate their criminal activities. Transportation and logistics will increasingly rely on the use of Big Data and cloud-based services, exposing these sectors to cybercrime. Cyber attacks are already a threat to private and public sector digital systems, but will also emerge as a major risk to physical business infrastructures and as-sets. OCGs involved in cargo theft will develop new innovative modi operandi to exploit auto-mated transportation systems. These groups will attempt to infiltrate or control systems for flight, rail or other modes of transport to divert the routes of automated vehicles in order to steal their cargo. This high-tech hijacking will allow criminals to steal high-value goods with-out the need to be anywhere near the crime scene.

OCGs will increasingly trade in data linked to transportation and logistics, providing valuable information to other criminals or to compet-itor companies. This data can be obtained by hacking and social engineering, as well as the physical infiltration of companies in the transportation and logistics sector. This data will include sensitive business information, personal data and intellectual property crucial to the infiltrated businesses. The outsourcing and provision of services by companies on a global scale will provide OCGs with more op-portunities to infiltrate longer logistics' chains allowing for the facilitation and/or concealment of trafficking activities.

Changes in transportation and logistics infra-structures will change how and where illicit goods, such as drugs, firearms, counterfeit goods, illicit waste or protected species, are trafficked. Some criminal markets will be displaced, giving way to new routes, hotspots and emerging criminal markets. Just as for legal goods, 3D printing will move the production of illicit goods closer to consumer markets. This is particularly likely for counterfeit goods, weapons and drugs, and may shift the focus to the trafficking of raw materials including illicit precursors.

The direction and types of flows of illicit goods are set to change. The use of previously inaccessible routes across the Arctic region will have an impact on the flow of commodities smuggled on a global scale such as drugs or endangered species. Due to its sophisticated transportation infrastructures and the emergence of new markets in Asia, the EU is likely to emerge as a transit region for various illicit commodities, connecting origin to destination countries across the globe. An exponential expansion of e-commerce will further intensify trafficking activities and the trade in illicit goods on a global level. The use of Unmanned Automated Vehicles for the trafficking of illicit goods will allow criminals to maintain merely a virtual link to their criminal activities. Law enforcement authorities will be challenged to identify or even detect suspects.

OCGs involved in the facilitation of irregular migration and the trafficking of human beings will seek to exploit changes in transportation and logistics. Criminals and victims will make use of a diversification of transport options. Irregular migrants may be transported in Unmanned Automated Vehicles used for land, sea and air travel without establishing personal contact with facilitators. Facilitators will seek to develop or buy the expertise to infiltrate transport control systems in order to provide access to transportation. Key hotspots as well as routes for illegal entry into the EU will change as a result of demographic changes and shifts in the economies of source and transit countries. As countries in Asia emerge as attractive destinations for migrants, the EU may develop into a transit region for irregular migration, or even a region of origin. These developments are also likely to affect the trafficking in human beings and its victims. The outsourcing or crowdsourcing of tasks in the logistics sector in order to decrease costs may provide new opportunities for labour exploitation.

The large sums of money associated with transportation and logistics projects in research and development, infrastructure and production are likely to increasingly attract financial and economic crime. OCGs will seek opportunities to defraud and corrupt tenders, public-private partnerships and infrastructure projects. It will become more difficult to control complex supply chains involving multiple modes of transport. Increased security measures, both those associated with supply chain security and customs, will most likely lead to delays in the processing of goods in transit, which may give rise to more corruption attempts intended to speed up clearance procedures. Logistics companies will provide additional advice on customs procedures and how to circumvent regulations. Some OCGs will specialise in providing services relating to the facilitation of transportation and develop business models to generate substantial profits from the circumvention of procedures.

Fundamental changes to transportation and logistics on a global scale will also alter the nature of OCGs exploiting these sectors. Greater mobility will enable criminals to commit crime anywhere, anytime, quickly and inconspicuously. Crowd-sourced apps will facilitate criminal activities. For instance, navigation apps using the real-time data of users to find the most efficient routes will allow criminals to become better at evading law enforcement attention. Technology such as the use of Big Data, remote hacking, the hacking of robots and automated systems could provide OCGs with a truly global reach whilst relying on a limited number of technical experts and maintaining a low profile at the scenes of crime.

OCGs will generally require a higher level of expertise to misuse available data for their criminal activities. They will need to recruit members with expertise in information technology or the resources to outsource specific activities to external experts. The move to the infiltration of control systems for transportation and logistics is likely to make violence a largely irrelevant tool for the OCGs involved, except at times to keep key facilitators and competitors in line.

> *Criminals will attempt to infiltrate or control systems for flight, rail or other modes of transport to divert the routes of automated vehicles in order to steal their cargo.*

18

Data as a commodity

The increasing exploitation of Big Data and personal data will enable OCGs to carry out complex and sophisticated identity frauds on previously unprecedented levels.

For sale: your data

The rise of Big Data and the emergence of the Internet of Everything, which merges devices, processes and data, have seen a dramatic increase in the quantity and quality of personal data collected by private companies, state authorities and criminal actors. Personal data is expected to become an increasingly valuable commodity; it will be ubiquitously collected and converted for the targeting of services in the business sector and be similarly exploited by criminals for the targeting of the services they supply, as well as for fraud. The growing wireless interconnectivity of products such as vehicles, home appliances and clothing, also known as the Internet of Everything, will offer a far wider range of opportunities to gather data on users. Product preferences, daily schedules, personal health and location are all expected to be continuously recorded as these devices are used. Additionally, the current usage of the internet and smart devices demonstrates that users are already willing to make personal data, such as their relationship status, employment history and images, available to third parties. It

is expected that this publication of information will increase as more devices ask for personal data input from their users. Legislators will be challenged to maintain the privacy rights of the users of these devices and it is expected that legislation will focus on the regulation of information collection, dissemination and monetisation rather than its prevention.

The data gathered through passive data collection by consumer products and active user input is used by product manufacturers and in many cases sold on to the advertising industry. In addition to data acquisition through interconnected devices, the collection of biometric data is also predicted to expand. Biometric information will become less expensive to gather and process. State authorities and the private sector will rely on biometric information for a wide range of purposes including identification technologies, forming social networks based on genetic similarities or using genetic information on predispositions for certain diseases to decide on the cost of health insurance policies [2].

Skimming your life

The increased collection and value of biometric and personal data will offer many opportunities for serious and organised crime. Cybercriminals are already able to gain large amounts of information on potential victims. Personal data is typically obtained by network intrusion or intercepting data transfers. However, cybercriminals may increasingly target databases belonging to product manufacturers and advertising

© Shutterstock

19

agencies. The data stolen from these sources can be sold to other criminal groups specialised in highly personalised scams. Information that will be useful for this purpose includes personal interests, social network structure and financial details. Additionally, increased interconnectivity will give criminals the opportunity to develop ransomware for essential products such as vehicles, refrigeration units or heaters.

Data may also be vulnerable to theft using contactless bank or credit cards. Radio-frequency identification (RFID) technology, allowing for purchases to be made by holding cards up to an RFID reader, is already used in Europe and will become common in shops and cafés due to the ease and speed of payment. This creates opportunities for a new type of skimming using RFID readers to copy card data. The card does not need to be used and can even be 'skimmed' through a wallet or clothes. OCGs may travel to busy locations such as public transportation hubs or popular stores and use concealed readers to gather the card information of oblivious passers-by. This information will then be used or sold on to other criminal groups. It is expected that the financial industry will take measures to prevent this form of skimming, although the extent of these measures may vary. Should contactless payment grow in popularity, measures such as skim-proof card covers or wallets are expected to be used.

Although current technology does not allow for mobile wallets to be effectively skimmed, near field communication technology that enables financial data to be stolen from mobile phones may be developed by criminals. It will then be used in the same way as contactless skimming.

Identity fraud will become more sophisticated as a result of developments in the collection of personal and biometric information. As the use of biometric data becomes widespread, it is likely that databases holding this information will be targeted by cybercriminals. The proliferation of biometric data as a means of authentication has the potential to make online services more secure. However, compromised biometric data may also pose additional risks. Traditional authentication mechanisms such as passwords or phrases can be updated by users if they suspect their accounts have been compromised. Biometric data are inherently constant and their exposure to cybercriminals may have more far reaching consequences than compromised passwords. Biometric data is often considered inherently reliable for authentication. Once compromised, biometric data could provide criminals access to physical structures as well as sensitive information.

Skilled cybercrime groups already provide full stolen identities to interested buyers, usually for use in the commission of various frauds. In the future, this data package will consist of even more comprehensive information including the biographical data, personal details, photos, credit card information and biometric data of an individual. It is expected that the trade in illicitly obtained information will increase as the utility of the data for criminals becomes higher. OCGs will benefit from these more comprehensive stolen identities in various crime areas. OCGs involved in the facilitation of illegal immigration and the trafficking of human beings can use this data to provide irregular migrants and trafficking victims with new identities complete with all the information necessary to avoid risk profiling or law enforcement countermeasures upon entry to the EU or during secondary movements. Similarly, OCGs involved in the trafficking of drugs using couriers will be able to buy and use identities that are unlikely to fall within risk categories. Some OCGs will provide specialised identity packages to order, tailored to specific modi operandi employed by OCGs in various crime areas. For instance, OCGs involved in the trafficking of endangered species may order identities linked to research institutions in order to ship specimens of endangered species using special permits only issued for scientific research purposes.

Nanotechnology and robotics

Nanotechnology and robotics will open up new markets for organised crime and deliver new tools for sophisticated criminal schemes.

Technology: the next generation

Nanotechnology refers to the branches of science and engineering which utilise phenomena taking place at the nanoscale [3] to design and produce smart nano- and micro-systems [4]. Current applications of nanotechnology are mainly within the areas of agriculture, medicine, information technology and environmental protection [5]. Nanotechnology and robotics are currently only used in highly specialised settings such as hospitals or research institutes and their application requires significant investment.

Nanotechnology in particular has not moved far beyond experimental settings. However, it is expected that technical innovation, especially in making nanotechnology and robotics part of widely-used consumer products, will result in significant reductions in the cost of manufacturing. This will create opportunities for nanotechnology to become mass produced, making nanoscale devices more widely available and affordable for the general public.

Robotics takes place on a far larger scale than nanotechnology. It is an area of engineering that involves the development, construction and operation of robots and the computer-based systems which drive them. The EU has invested in over 120 robotics projects in order to develop a range of products and services in the medical, manufacturing and surveillance industries [6].

Developments in the areas of robotics and nanotechnology will have a significant impact on European society. Several activities are already performed by robots within the manufacturing and health industries, and rapid improvements in robotics are expected, leading to robots performing tasks of higher complexity. Labour markets will be able to rely on fewer employees which may result in increased profits, but can also create social unrest. Robots are expected to be utilised frequently within healthcare environments, to provide for the elderly and assist during surgery.

Technological advances within the field of nanotechnology will take place at a slower rate due to the difficulty of development, but its impact on society is expected to be substantial. Nanotechnology will be increasingly used within medical and informational contexts. Improvements within nano-computing will allow for extremely small electronic devices to be capable of advanced computation. This will enable all types of products, even contact lenses or clothing, to be used for information gathering and processing. Maintaining privacy and informational security will become increasingly difficult as devices containing nano-computers become widely available.

Nanotechnology for macrocrime

Robotics and nanotechnology will also impact on serious and organised crime. The increased dependence of the manufacturing and healthcare industries on robotic workers will create vulnerabilities that can be exploited by criminals. The ability to hack the workforce of a factory or hospital offers new opportunities for computer-based extortion. However, the high level of technical expertise that is required makes it unlikely that many OCGs will be capable of robotic hostage taking. It is expected that this type of crime will be committed for

political reasons rather than for profit and that it will be the domain of very few lone actors possessing significant expertise in this area. Robotic workers will also provide opportunities for law enforcement. They are expected to be used to support police forces in all areas of their functioning. Bomb disposal, traffic policing and surveillance are examples of tasks that are likely to be delegated to robots.

The complexity and cost of nanotechnology offers high barriers for entry to both law enforcement and OCGs. It is vital that law enforcement agencies invest the necessary time and budget to obtain the knowledge required to respond to nanotechnology-based threats and opportunities. Nanoscale technologies are expected to become as ubiquitous as personal computers, and failure to develop law enforcement capabilities to address this developing area will create a blind spot that can be exploited by OCGs.

OCGs in possession of the necessary funds will use nanotechnology to develop or alter psychoactive substances. They may take advantage of the developing market in nanotechnologies to produce counterfeit drugs or devices. Nanotechnology also provides an area of opportunity for law enforcement agencies through the improved sensory abilities of scientific instruments. The ability and the speed with which forensic scientists will be able to examine crime scenes and traces left by criminals will increase greatly, because nanotechnology will allow for faster DNA analysis and highly detailed examinations of fingerprints and blood samples.

100

NEARLY 100 MILLION TONNES OF E-WASTE BY 2017

GREEN E-WASTE

"

An exponential increase in the quantity of e-waste has the potential to result in the emergence of e-waste as a major illicit commodity rivalling the trafficking of drugs in terms of scale and profits.

22

E-waste

Without the necessary legislative and law enforcement responses, the illicit trade in e-waste is set to grow dramatically in the near future both in terms of quantities traded and the quality of the methods used by criminal actors engaging in this activity.

From waste to gold

The output of waste in Europe has increased dramatically over the past 30 years. While the quantities of household and industrial waste are increasing fast and have prompted the development of large and sophisticated waste management industries, one particular type of waste combines unprecedented growth potential with value as a traded commodity – electronic waste.

An increasing reliance on technology in all areas of life is driving an ever-increasing pro-liferation of electronic devices in households, workplaces and public spaces. Technological progress, built-in obsolescence and much higher replacement rates for consumer devices have led to the shortening of device life spans, generating an exponential growth in e-waste in the form of discarded devices and spare parts. There is a wealth of literature detailing the rap-id increase in the number of obsolete electronic devices, as emerging markets in China, India or Brazil feature huge and growing demand and the average life-span of an electronic device

decreases rapidly. Conservative estimates see the total number of obsolete PCs and phones in developing regions of the globe outstripping that of developed regions by 2017. In 2012, an estimated 48.9 million tonnes of e-waste were generated. [7] This represents a growth of 15.2% compared to the global quantity of e-waste dis-carded in 2011. [8] Even if current growth levels of e-waste generation are maintained on a year to year basis, by 2017 the annual global output of e-waste is estimated to range from 65.4 mil-lion tonnes [9] to 93.5 million tonnes. [10]

These projections cannot take into account the emergence of new technological trends. For instance, it would have been difficult to con-ceive just 10 years ago that demand for smart phones and tablet computers would signifi-cantly outstrip desktop computers. The results of such trends in the future are likely to result in even higher growth potential for e-waste generation.

Perhaps more than any other development over the past 50 years, advances in technolo-gy have sustained economic growth, shaped industrialised societies and had a profound impact on the environment. E-waste is one of the by-products of these developments and threatens to emerge as a key criminal commod-ity of the future.

A key illicit commodity of the future

The phenomenon of waste trafficking is not a new one. Criminal groups such as Italian mafia organisations and OCGs in eastern Europe have a long tradition of being involved in

© Shutterstock

23

the business of illicit 'waste management'. Traditionally, waste trafficking involved the disposal of household and industrial waste at lower prices than legal waste management providers, by circumventing legislation intended to ensure environmental protection and fair competition.

The quantity of e-waste is set to increase substantially over the next decade and OCGs will increasingly seek to exploit this resource. The proliferation of electronic devices containing precious metals and materials such as gold, silver, nickel and palladium has already turned e-waste into a valuable commodity that is traded, bartered and trafficked on a global scale like other illicit commodities such as drugs, firearms or endangered species. The two driving factors behind the emergence of e-waste as a key illicit commodity of the future are scale and profits. These two elements perpetuate a dynamic cycle that feeds off the scarcity of the materials required for the production of every-day electronic goods, for which demand is rising across the globe, as well as the abundance of the electronic waste containing these precious resources.

OCGs are already heavily involved in the trafficking and trade in e-waste, which promises substantial profits and often only entails the low risk of being fined a modest fee if discovered. However, an exponential increase in the quantity of e-waste has the potential to result in the emergence of e-waste as a major illicit commodity rivalling the trafficking of drugs in terms of scale and profits.

Currently, e-waste originating from the EU is frequently shipped to West Africa and India. An expansion of the market in e-waste is likely to be accompanied by a diversification of destination regions where the waste is processed. This may even result in the emergence of mid-scale

illicit processing of e-waste in Europe. Similar to the use of clandestine laboratories for the production of synthetic drugs today, OCGs may establish processing facilities for e-waste resulting in serious environmental damage to the affected areas and significant health risks to local populations.

Africa and Asia in particular are emerging as major producers of electronic waste themselves and it is likely that the processing of e-waste will develop as a major industry in these regions. The impact of advanced global transport infrastructures on organised crime is described in a separate chapter in this report. However, it is clear that the shipment of waste across continents in ever greater quantities will attract some degree of organised crime involvement.

OCGs may also seek to profit from e-waste generated from sources other than household consumer electronic devices. Solar panels are increasingly becoming a mainstream source of energy, whether included in the construction of new building developments or added on as part of renovation projects. While solar panels are increasingly widespread throughout the EU, there is as yet no clear recycling or waste stream for them. [11] Organised crime has already invested heavily in 'green energy' generation as part of various schemes involving subsidy fraud and has direct access to green energy as-sets through various legal business structures. OCGs are likely to attempt to profit from the trade in end-of-life green energy infrastructure as many of these installations contain the same metals and resources found in other e-waste products.

The trade in and trafficking of e-waste will increasingly attract OCGs in the EU and beyond. Without the necessary legislative and law enforcement responses, the illicit trade in e-waste is set to grow dramatically in the near future both in terms of quantities traded and the quality of the methods used by criminal actors engaging in this activity. The processing of illicit e-waste is environmentally harmful and has already resulted in significant environmental damage. It also entails serious dangers to the health of populations exposed to the toxic by-products of e-waste processing. The trade in e-waste by organised crime is a major criminal threat and challenges the Member States of the EU to cooperate with partners on a global scale in order to combat the emergence of e-waste as a key criminal commodity of the future.

Economic disparity within the EU

Economic disparity across Europe is making organised crime more socially acceptable as OCGs will increasingly infiltrate economically weakened communities to portray themselves as providers of work and services.

Mind the gap!

Income disparities within the EU [12] and its Member States are substantial and expected to increase significantly in the future. Employment no longer guarantees protection against poverty as precarious forms of work such as temporary contracts are becoming the new norm [13].

Recovery from the financial crisis is expected to be slow and it is unlikely that the EU will reach its pre-2008 growth rate of around 5% before 2025 [14]. The process of debt reduction will be protracted and varied across different Member States. Long-term low inflation increasingly appears to be a considerable risk [15] to growth and employment.

However, the EU and its Member States are pursuing policies intended to foster sustainable and inclusive growth [16]. While economic policies vary from Member State to Member State, most efforts aim at increasing labour productivity, creating employment and enhancing the attractiveness and competitiveness of European markets. In practice, this has entailed structural reforms as well as financial incentives intended to strengthen the industrial sector, promote innovation and ensure resource efficiency.

Despite a recent slow-down, the growth in emerging markets and developing economies is expected to further increase in the mid-term. China's economy continues to grow [17] . The economic gap between emerging and advanced markets is closing rapidly and will result in significant shifts in the global economic landscape by 2025. The share of financial assets held by emerging markets is expected to almost double by 2020 [18] and China is expected to overtake the United States as the world's largest economy before 2030 [19] [20] . These developments might make Europe less attractive to external investors, which would result in a further reduction in GDP growth, greater unemployment and widening income disparities within the EU.

An organised crime climate

OCGs of the future are adaptable and quick to exploit changes in their environment, especially changes in the economic landscape, by identifying new markets, offering new services or devising new modi operandi. The growth of the middle classes in emerging economies such as China, India, Brazil and Russia will create new opportunities for serious and organised crime. These middle classes represent a vast market for illicit commodities as well as potential targets of choice for both legal and illicit investments, and for professional fraudsters. Middle classes in emerging markets will represent a market of up to 2 billion additional consumers by 2030 [21]. Currently, less than 1 billion people account for three quarters of global consumption. The anticipated massive expansion of the global consumer base will trigger a major increase in the demand for all types of goods and services, both legal and illegal. OCGs will be able to benefit from this development across a range of different crime areas including the trafficking of drugs, the trade in counterfeited goods, MTIC/VAT fraud, excise tax fraud, advance fee fraud and payment card fraud.

Meanwhile, declining prosperity in some parts of Europe may force OCGs to adapt to a consumer base that is able to spend less on the illicit commodities they are offering. The drugs market will continue to be driven by

25

the dynamic relationship between the cost and effect considerations of consumers and the supply-side availability of drugs. However, market shares of specific drugs are expected to change significantly as the demand for cheaper and more 'effective' drugs will dominate the market. Demand for synthetic drugs including New Psychoactive Substances (NPS) is expected to increase significantly, while cocaine and heroin will become less popular. The demand for counterfeit goods may increase substantially, as a larger part of the population will have to rely on diminishing disposable income. Economic hardship might make the reliance on illicit products such as counterfeit every-day products more socially acceptable and services and products offered by OCGs might be increasingly perceived as legitimate alternatives. OCGs producing counterfeit goods may also increasingly rely on illegal labour exploitation to bolster their workforce in order to cope with the growing demand for their products.

Economic decline in many EU Member States is likely to change patterns of organised crime activity. Instead of targeting countries in western Europe, mobile organised crime groups may increasingly focus their activities on eastern Europe where economic development and increasing prosperity offer many opportunities for entrepreneurial organised burglars and car thieves.

Poverty and declining prosperity provide fertile ground for criminal exploitation. Economic disparity in the EU may result in an increase in facilitated immigration and the trafficking in human beings for exploitation in labour, the sex trade and forced criminality. Demand

for cheap labour is bound to rise significantly as a result of a rapid expansion of the global consumer base, resulting in more labour exploitation in traditionally affected industries such as hospitality, construction or cleaning services. Industries not typically associated with this phenomenon may also be targeted. In the future, labour exploitation may take place in the context of new and emerging business models such as crowd-sourced initiatives or rapidly expanding sectors such as e-commerce. Economic decline may also expose new groups of victims and professions to potential victimisation. For instance, the large-scale outsourcing of administration may be accompanied by the exploitation of trained and qualified individuals in book-keeping, data entry or any other service which can be provided remotely online.

The patterns of exploitation in the EU are already changing as a result of economic pressures. Victims of sexual exploitation are increasingly trafficked within the EU and it is conceivable that sustained or growing economic disparities within the EU may prompt a similar shift to intra-EU trafficking for labour exploitation and exploitation in forced criminality. EU citizens with very low incomes or experiencing a substantial decline in their living standards will become increasingly vulnerable to such forms of exploitation, including advance fee frauds offering employment and working conditions that appear more favourable than those available in the legal labour market. Declining prosperity in Europe and the proliferation of wealth in emerging economies may also prompt more EU citizens to emigrate. It is conceivable that OCGs will begin to offer comprehensive facilitation services for EU citizens

> *EU citizens with very low incomes or experiencing a substantial decline in their living standards will become increasingly vulnerable to exploitation, including advance fee frauds.*

seeking to illegally enter new destination countries in Asia or South America. Europe may still remain a destination region for irregular migrants from less prosperous regions, but it may not necessarily remain in the top tier of desired destination regions.

Economic decline is likely to entail a rise in petty, non-organised forms of criminality including social benefit fraud or theft. These activities will also be carried out by OCGs masking their activities as petty criminality but orchestrating large-scale criminal enterprises with complex structures. The potential emergence of a culture of distrust is particularly threatening and could benefit OCGs by undermining citizens' trust in the authorities and increasing the appeal of organised crime as a provider of goods and employment.

Socio-economic disparities are a crucial factor in the spreading of social unrest and disorder. Historical examples for the link between disparity and unrest include the so-called "IMF riots" in the 1980s and 90s. Austerity measures such as cuts in welfare payments or subsidy cuts for basic commodities such as food [22] or water [23], profoundly undermined citizens' trust in their governments. The failure of states to guarantee minimum standards of living has been shown to spawn a myriad of social movements and initiated a wave of violent protests. Some similar developments can be noted in Europe today. The economic crisis has given rise to social movements questioning state authority and promoting open democracy including 'Indignados' and the 'Occupy' movement. Forms of protest and technological progress have been converging to enable movements to be organised entirely

in the virtual realm. The tools developed by some of the most radical supporters of these movements have the potential to cause substantial harm in the near future. Technologies being developed by crypto-anarchist groups could be of great benefit to OCGs, especially with further refinement. Innovation towards self-replicating 3D printers will make 3D printing widely available and could potentially offer new opportunities for OCGs involved in firearms trafficking or the trade in counterfeit goods. Alternative cryptocurrencies with anonymity as their core feature such as Darkcoin and various Bitcoin laundering services such as Bitcoin Fog or Dark Wallet will make transactions practically untraceable, heavily facilitating the trade in illicit goods online.

Violent radicalisation and organised crime intersect and interact in the wider criminal economy. Tools developed under the pretext of social resistance also aid criminal activities, sometimes by design. Some violent radical groups and lone actors use their ideologies to rationalise or conceal the criminal intent and profit-driven nature of their activities. The economic crisis and widely felt declining prosperity has afforded these groups with visibility and the opportunity to recruit new members, amplifying their threat potential.

Difficult economic circumstances will attract some individuals to serious or organised crime. Declining prosperity and a lack of income alternatives provide OCGs with a larger pool of potential recruits. Sustained economic problems are likely to make organised crime and OCGs more socially acceptable and create an environment that promotes corruption.

27

OCGs will increasingly attempt to infiltrate industries depending on natural resources to act as brokers or agents in the trade with natural resources.

Fuelling the future of organised crime

With a significant rate of population growth and increasing per head consumption of energy, food and goods, countries around the world will find their access to natural resources increasingly limited. The infiltration of multi-national companies may enable OCGs to control access to natural resources and generate unprecedented profits. Some markets for essential natural resources are dominated by monopolies or oligopolies, which amplifies the potential threat posed by OCG infiltration of these market-dominating global corporations. Most natural resources are found outside the EU, so EU-based OCGs may not directly control these resources, but may find niches for themselves by increasingly acting as brokers or agents, for example for companies seeking drilling rights or access to pipelines.

Oil

A race has begun for control over resources in the Arctic Ocean and Antarctica. Access to the Antarctic region is currently governed by the Antarctic Treaty, which came into force in 1961 and protects the continent as a scientific preserve. The Treaty will expire in 2048 and it is possible that energy-hungry countries will opt not to renew it and instead compete for the extraction of a projected 200 billion barrels of oil. Access to oil reserves in the South China Sea is also currently hotly contested between the Chinese and Vietnamese governments and this dispute is expected to continue.

OCGs will seek out various opportunities to become involved in this sector. Increasing oil prices will make oil siphoning from pipelines, filtering or washing of industrial grade diesel for road use, VAT and excise frauds profitable activities for OCGs. They will also increasingly engage in cybercrime in attempts to gain control over critical infrastructures. Some OCGs are already involved in these activities. However, in the future, it is expected that many more OCGs will seek to enter and intensify their involvement in this sector resulting in increased competition between groups.

International oil companies are already exploring oil reserves in the Balkans and the deep trench basins surrounding the continent of Africa. High levels of corruption in both regions provide fertile ground for OCGs to infiltrate the supply and maintenance of pipelines and other types of infrastructure.

Gas

Similar to oil, gas is a highly valuable commodity. Natural gas reserves are being tapped with new 'fracking' [24] technology, which has led to a glut and low prices, especially in the United States. Liquid natural gas cannot be transported easily; large infrastructure projects in the United States aim to facilitate the transportation and export of liquid natural gas by train and ship. OCGs may become involved in the building and maintenance of this infrastructure in order to control access to and supply of critical resources. Ports are particularly at risk of OCG infiltration and there have been precedents of these activities such as the Camorra's control over the port of Gioia Tauro in Calabria, Italy.

Energy security has emerged as a significant concern to the EU and its Member States are exploring alternative sources of energy in response. The United States have committed themselves to establishing the infrastructure necessary to export liquid natural gas in the event of a complete pipeline shut-off as soon as possible.

> *OCGs may become involved in the building and maintenance of large infrastructure in order to control access to and supply of critical resources.*

The high-level infiltration of power companies by OCGs remains a significant concern to EU Member States. OCGs may also increasingly seek out criminal opportunities in price rigging and the black market supply of both oil and gas.

Water

Water is becoming an increasingly scarce resource, which is already a significant issue in South Asia. The region's population is projected to rise by 32% over the next 30 years. Competition for resources is expected to increase and become a major issue driving country policies and dominating international relations in the region. Climate change is likely to make water scarcity a problem for many regions across the world.

OCGs are likely to attempt to profit from the scarcity of valuable resources such as water by siphoning or stealing water and selling it on for exorbitant prices. OCGs are already involved in the siphoning and stealing of oil and gas directly from pipelines and could easily extend these activities to the theft of water. OCGs are liable to use the corruption of employees of water companies to gain access to water.

Food

Food prices are inextricably linked to oil prices. However, food prices are also affected by drought and floods. Changes in global weather patterns are likely to result in more frequent droughts and floods, which also have a significant impact on fluctuating food prices.

Spikes in food prices in 2008 were considered to be one of the factors influencing social unrest in the Middle East. [25] During the Arab Spring in 2011, prices spiked again causing unrest in Algeria, Bahrain, Egypt, Iraq, Libya, Mauritania, Oman, Syria, Saudi Arabia, and Uganda.

OCGs may attempt to capitalise on the scarcity of food and rising food prices. It is possible that OCGs with large resources start to stockpile food supplies to sell on black markets in future. OCGs are likely to increasingly engage in the diversion and theft of cargo containing food and other valuable supplies. UN aid supply trucks have been targeted and raided by armed groups in the past. Such incidents may multiply in the future and increasingly affect regular supply routes rather than only aid shipments in conflict zones.

Food scarcity would likely entail a degradation of the overall quality of foodstuff available to consumers in Europe. In the EU, OCGs will likely exploit growing demand for good-quality food by increasingly engaging in food fraud. This could entail the repackaging or relabeling of low-quality food as high-quality products. OCGs may also increasingly produce and distribute low-quality food products themselves.

Land for agricultural use will continue to become an increasingly valuable resource. OCGs may attempt to gain control over food supplies and food supply chains by buying up farm land. This type of activity would enable OCGs to generate substantial profits and exert pressure on citizens and state institutions alike. Food security is an essential requirement for the functioning of societies and the undermining of this essential provision is a particularly threatening scenario.

© fotolia.com

29

The proliferation of virtual currencies

Virtual currencies increasingly enable individuals to act as freelance criminal entrepreneurs operating on a crime-as-a-service business model without the need for a sophisticated criminal infrastructure to receive and launder money.

Paying in Bits

The emergence of virtual currencies [26] has been the subject of intense debate in the media and among law enforcement authorities [27]. Currently, numerous virtual currencies enable anonymous payments on the web. While Bitcoin is the most popular cryptocurrency [28], to date there is no universally accepted virtual currency. However, virtual currencies are set to become more user-friendly and accessible to a wider pool of potential customers. This development may entail the emergence of one or several key virtual currencies accepted across platforms and e-commerce sites. The proliferation of payment operators automatically processing transactions made by different currencies could also support diversification.

Virtual currencies offer a particular set of features that make them attractive to criminals: anonymity or pseudonymity, and the rapid and irreversible transfers of funds. Although generally designed for legitimate use, virtual currencies are heavily abused by criminals. Criminals often favour centralised schemes (particularly for criminal-to-criminal payments) which are inherently more stable compared to cryptocurrencies whose price is highly volatile.

Virtual currencies are an ideal instrument for money laundering. Entry to and exit from the system is via an exchanger. Exchange services are another niche service offered in the digital underground economy. However, legitimate exchangers are also exploited, particularly those which do not apply Know Your Customer (KYC) principles and offer multiple methods to 'cash out' including payments via pre-paid or virtual credit cards and Money Service Bureaus.

Once in control of the digital funds, the ease of creating new e-wallets means a launderer can easily discard 'dirty' wallets. In addition to traditional layering methods, cryptocurrencies use specialised laundering services known as 'tum-blers' or 'mixers' to obfuscate transactions to the point where it is very resource intensive to trace them.

Unregulated or inadequately regulated online gambling has been exploited for money laundering purposes for years. The introduction of the possibility to pay, play and cash out using virtual currencies has however added a new level of anonymity.

"

The role of freelancers in organised crime is expected to become more prominent as a result of the thriving anonymous market.

Virtual currencies for real crime

Virtual currencies have already had a significant impact on various types of criminal activity facilitating the exchange of funds between criminal actors and giving rise to a flourishing black market economy on Darknet marketplaces. However, it is anticipated that virtual currencies will expand their user base and will be used increasingly for transactions outside the virtual realm. Virtual currencies have the potential to emerge as the preferred method of payment across various crime areas including traditional ones such as drug trafficking, the sale of counterfeit goods or illicit firearms.

While decentralised virtual currencies or cryptocurrencies have been less popular with cybercriminals, they have become the currency of choice for internet-facilitated traditional crime on the Darknet. Darknet marketplaces typically use Bitcoins as a method of payment.

As virtual currencies continue to evolve, it is likely that more niche currencies will develop, tailored towards illicit activity and providing greater security and true anonymity. Schemes such as MUSD, the United Payment System and UAPS have been developed to cater specifically for these markets. Proliferation of these schemes will permit an entire criminal economy to flourish with little possibility of law enforcement intervention.

The role of freelancers in organised crime is expected to become more prominent as a result of this thriving anonymous market. Individuals with computer expertise and other skills that are valuable to criminal organisations are expected to advertise their services for payment in cryptocurrencies. If a freelancer is apprehended by law enforcement, the anonymity of the payment means there will be no money trail to follow back to the larger organisation. This will allow criminal groups to outsource specialised activities at little risk to themselves.

Groups dealing with trafficking in human beings, firearms and drugs will increasingly make their services and goods available on illicit marketplaces. Sex trade and the sale of drugs are expected to make up the bulk of the business. The anonymity afforded to the buyer by the use of cryptocurrency may lower the entry barriers for members of the general public to become involved in the online purchase of illegal materials.

A number of malware variants on both PCs and mobiles include e-wallets in the data they harvest from infected devices. Other variants turn their hosts into cryptocurrency miners, using the devices' processing power to generate freshly mined coins for the attackers. We can only expect to see this becoming more commonplace.

31

Demographic change in the EU

OCGs will increasingly target but also provide illicit services and goods to a growing population of elderly people exploiting new markets and opportunities.
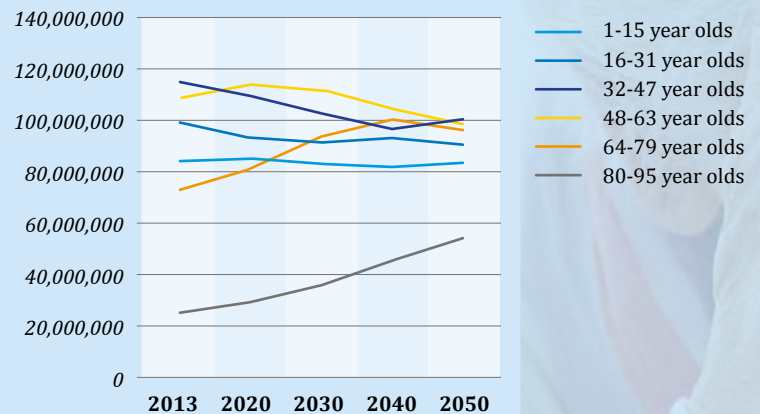
Rise of the silver citizen

Demographic change in the largest Member States of the EU and the wider industrialised world has been a subject of debate since the late 1990s. The average age of citizens of highly industrialised societies has been increasing and is projected to continue to do so. This development will result in larger populations of elderly people in many EU Member States.

Globally, people are living significantly longer than in previous decades. Life expectancy has increased by two decades since 1950, from 48 years in 1950–55 to 68 years in 2005-10. By 2050, the UN Population Division projects global life expectancy to rise further to an average of 76 years. [29] This global development is even more apparent in Europe. The number of Europeans aged 65 and older has tripled over the last sixty years and the number of people aged 80 years and older is six times higher than in 1950. According to the medium scenario of the UN population projections, population aging will continue in future decades. By 2050, the number of people older than 65 is expected to be 55% higher than today and the number of people older than 80 is expected to double. [30] EU figures project a growth in population over the next 30 years, but the elderly will make up a growing segment of this population. Birth rates in many EU Member States and the EU as a whole have shown a trend of continuous decline over the past three decades. [31] This development is already resulting in an increase in the average age of EU citizens and it is projected that this trend will continue for the foreseeable future.

Projected Population Figures for EU 28 by Age Group

Source: Eurostat

Legend:
- 1-15 year olds
- 16-31 year olds
- 32-47 year olds
- 48-63 year olds
- 64-79 year olds
- 80-95 year olds

Such a radical transformation of the demographic makeup of Europe will have a significant impact on the economies, societies and politics of affected countries. Labour markets will need to adjust to rely on fewer young employees and accommodate increasing numbers of employees at the end of their career, who would previously have retired were it not for recent changes to pension ages. Consumer and service industries will develop more products and services geared towards a substantial and growing consumer group of elderly people with very varied level of disposable income. This will have an effect on the nature of the products themselves and on the marketing of these offerings. Demographic change is impacting on family structures and modes of living with more elderly people relying on fewer young people for care and support. This is leading to a decrease in reliance on traditional family support and even greater dependence on private or public care providers. A larger percentage of people of an advanced age will also afford this group more political influence and is likely to result in more policies serving the interest of this growing segment of the population.

Old Europe – New criminal markets

Large-scale demographic shifts will also impact on serious and organised crime. Because of their vulnerability, elderly people have long been the targets of criminal activity and this is set to increase with a growing population of people aged 60 and above. Fraud against the elderly perpetrated by OCGs currently affects most EU Member States and is likely to spread more widely with a growing elderly population. However, the expansion of this section of the population not only constitutes a growing pool of potential victims, but also the emergence of a potentially significant consumer group for illicit commodities or services.

Elderly people are already targeted by OCGs as part of various fraud schemes. However, as a growing demographic of elderly people rely on income from pension schemes and social benefits, OCGs will increasingly engage in various forms of fraud against pension schemes and social benefit systems. These fraud schemes will either abuse elderly citizens to illegally obtain funds or provide unregulated advisory services to customers seeking to supplement their income with higher pension or social benefit payments.

The economic crisis has demonstrated that OCGs producing counterfeit goods are highly flexible and adaptable. Prior to the economic crisis, most counterfeits were copies of luxury items such as handbags, glasses or other expensive items. However, in response to decreasing levels of disposable income, OCGs have increasingly produced counterfeits of daily consumer goods such as washing powders or toothpaste. In the future, OCGs producing counterfeit goods are likely to attempt to specifically market their products to a growing target group of elderly customers.

Increasing age is often accompanied by an increasing reliance on pharmaceuticals and medical equipment. The proliferation of counterfeit medicines is already a major threat to the health of citizens of the EU and OCGs are likely to widen the range of counterfeit medicines to profit from the market for counterfeit medicines and medical equipment targeted at elderly people.

Some OCGs actively attempt to infiltrate and dominate profitable sectors of the economy. Examples of this include the creation or infiltration of businesses in hospitality, transportation, the construction sector or waste management. Healthcare provision is an increasingly profitable service industry that is likely to expand over the coming years, partially as a result of demographic change. Healthcare services aimed at providing care for the elderly represent a growth sector and OCGs may be tempted to enter this lucrative business. Infiltration of the healthcare industry by organised crime entails the risk of sub-standard care provision to vulnerable members of society and also offers additional opportunities for criminal activities such as the proliferation of counterfeit medicines or various fraud offences against patients and insurance providers. This development is the likely result of an anticipated drive by OCGs to move increasingly into the area of service provision, which promises significant profits, a lower risk of detection and much lower penalties than traditional criminal activity.

The aging of Europe's population is set to have an impact on the criminal landscape in the EU. Elderly people will increasingly be targeted for fraud offences, but may also emerge as a significant consumer group for illicit commodities. OCGs may want to take advantage of an expanding health sector by extending their activities to involve different aspects of care provision and intensify their involvement in the manufacturing and distribution of counterfeit pharmaceuticals. Overall, demographic change is not likely to impact quantitatively on serious and organised crime in the EU, but it will cause shifts in commodity markets and open new criminal opportunities for OCGs ready and willing to adapt to the changing make-up of Europe's population.

THE EVOLUTION
OF CRIMINAL

Considering the development of serious and organised crime as a whole and the impact of key drivers, today's criminal markets can be classed in three distinct categories:

© fotolia.com

1 **Dynamic or growing criminal markets** are expected to develop over the next years. The most dynamic markets are not always the largest. Nonetheless, they challenge law enforcement authorities with quickly evolving modi operandi, new and previously unknown substances or the use of technologies which may only be at a concept stage today.

2 **Stable criminal markets** are sustained by established criminal activities that rely on tried and tested modi operandi supporting highly profitable business models. Established routes, highly developed modi operandi and continuing demand for illicit commodities in the EU and beyond will mean that these criminal markets will persist and continue to challenge law enforcement authorities. These markets represent the largest share of serious and organised crime in the EU currently and will continue to do so in the future.

3 **Criminal markets in decline** are expected to diminish over time as commodities change or certain criminal tools become less relevant in a digital age.

Synthetic drugs and new psychoactive substances

Counterfeiting of goods

Cybercrime

Environmental crime

34

MARKETS

Cannabis

Facilitation of illegal immigration

Trafficking in human beings

Organised property crime

Fraud

Trafficking in firearms

Currency counterfeiting

Cocaine

Heroin

The most dynamic criminal markets

Europe's criminal landscape is comprised of a diverse range of individual criminals, loose networks and OCGs operating across various crime areas ranging from traditional activities such as drug trafficking to emerging and quickly developing fields such as cybercrime. Europol monitors these crime areas closely and reports regularly on their evolution in its flagship product, the Serious and Organised Crime Threat Assessment (SOCTA). While all the crime areas reported on in the SOCTA have a serious impact on the EU, its Member States and citizens, certain criminal markets are expected to be particularly dynamic in nature.

The most dynamic markets are not always the largest. Nonetheless, they challenge law enforcement authorities with quickly evolving *modi operandi*, new and previously unknown substances or the use of technologies which may only be at a concept stage today. This section aims to highlight those crime areas, which are expected to be subject to the most significant change. It does not attempt to provide an assessment of their impact, harm or overall significance relative to other criminal threats.

Synthetic drugs and new psychoactive substances (NPS)

Synthetic drugs will continue to constitute a major problem in the EU. Traditional synthetic drugs such as amphetamine, methamphetamine, MDMA and other substances will remain available on the European drugs market and OCGs will continue to produce these drugs in the EU. However, law enforcement responses and legislative changes will prompt OCGs involved in the production of these drugs to innovate, resulting in better technology and more sophisticated production techniques. Recent experiences have shown that crime groups are able to respond quickly to the banning of precursor substances by shifting to non-controlled pre-precursors. As pre-precursor substances are banned, OCGs will move to alternative substances sustaining a perpetual dynamic between criminal innovation and law enforcement response.

New psychoactive substances (NPS) are likely to emerge as the most significant drug-related issue in the EU in the near future. The production and sale of NPS in many cases is a legal grey area, a situation which will continue to benefit distributors and encourage consumers rather than inhibit production and trade. Non-controlled NPS are easily imported to and distributed in the EU, servicing the demand of a rapidly increasing base of consumers in all Member States. NPS are already increasingly taking over a share in traditional drugs markets offering substances mimicking traditional drugs such as cocaine and heroin.

Online shops and global distribution infrastructures make it increasingly easy for individual users to obtain NPS and other substances to order. Open online trading in NPS is likely to increase expanding the consumer base for these substances. The market in NPS has the potential to grow dramatically and even rival the consumption of cannabis. Social acceptance of NPS is currently relatively high and may even increase with the emergence of widely consumed and popular NPS on the market. Eventually, millions of users may be able to order NPS anonymously from their home. New varieties of NPS will continue to emerge in significant numbers each year, potentially making this a key issue for law enforcement and public health authorities in the EU.

In June 2014, Europol supported the arrest of 6 Hungarian suspects belonging to an international organised criminal group responsible for the production and distribution of new psychoactive substances (NPS). Significant amounts of NPS, powders, herbals, crystal substances and relevant equipment were seized.

A tableting unit was dismantled and equipment to produce NPS (pentedrone) was seized and at other locations in Budapest many other products related to the production and distribution of new psychoactive substances were found. The production of NPS in the EU is still rare, but expected to increase over the next years.

Europol, June 2014

© fotolia.com

100 MORE THAN 100 NEW NPS EACH YEAR

© Shutterstock

"

3D printers may result in a shift to increased production of counterfeit goods in the EU

Counterfeit goods

Counterfeit goods will be sold almost exclusively online in the future. Online marketplaces for counterfeit goods will become even more sophisticated, replicating the original rights-holders' e-commerce sites and making it harder for consumers to distinguish between genuine and fake offerings. Greater awareness and protection of intellectual property rights in China will likely result in a shift to production zones in Africa.

3D printing will have far-reaching legal implications for intellectual property protection and will challenge law enforcement with new forms of counterfeiting, which will be very difficult to prove. It is possible that criminal organisations will become involved in the supply of counterfeit raw materials for 3D printers as well as counterfeit 3D printers and their components. 3D printers may result in a shift to increased production of counterfeit goods in the EU.

In terms of reduced access to resources, such as water and agricultural land, it is likely that adulteration of food stuffs with genetically modified products, as well as adulterated or counterfeit seed stocks, will become more commonplace to keep up with consumer demand.

An ageing population in the EU will lead to a rise in the production and trafficking of counterfeit pharmaceuticals, medical devices, artificial limbs as well as counterfeit vaccines. Europe's obesity epidemic may also prompt the distribution of more counterfeit slimming pills, diabetes treatments, related devices and heart medications. Online pharmacy business models are already highly successful and might be replicated for the sale and distribution of other counterfeit products.

There are already cases of counterfeit airbags and brake pads in the EU. These tend to be purchased online. In some cases, airbags that have deployed are re-fitted and re-used in vehicles, posing significant health and safety concerns.

37

© Shutterstock

Cybercrime

Technological innovation is rapid and in many cases unpredictable. Far from being limited to the virtual realm, cybercrime has been expanding to affect virtually all other criminal activities. The emergence of crime-as-a-service online has made cybercrime horizontal in nature, akin to activities such as money laundering or document fraud. The changing nature of cybercrime directly impacts on how other criminal activities, such as drug trafficking, the facilitation of illegal immigration or the distribution of counterfeit goods are carried out. The pace of technological development and the rapid adoption of new *modi operandi* and techniques by OCGs make it impossible to provide a detailed outlook on the future of this crime area. However, a number of significant trends are emerging now that will have a lasting impact.

General trends for cybercrime suggest considerable increases in scope, sophistication, number and types of attacks, number of victims and economic damage. Cybercrime is driven and facilitated by a service-based, commercialised criminal industry, exploiting a number of legitimate tools and services such as anonymisation and encryption. This allows traditional OCGs to carry out more sophisticated crimes, buying access to the technical skills and expertise they require.

It is to be expected that malware developers will increasingly target Internet of Everything devices and new forms of critical infrastructure. Malware will make more use of encryption and become increasingly 'intelligent'.

The use of new and more complex methods of social engineering can also be expected, exploiting for instance advances in the field of artificial intelligence. As more consumers progressively favour social media as a means of communication, it can be assumed that social media will be increasingly used to deploy and propagate malware.

Card-not-present fraud will increase proportionally with the growing number of payment transactions online. The proliferation of contactless payment systems will inevitably make them subject to attacks.

As virtual currencies offer features that make them attractive to cybercriminals, legitimate schemes will continue to be used and abused. It is expected that virtual currencies will continue to evolve, providing niche currencies for cybercriminals.

Evolved threats to critical infrastructure and human implants will increasingly blur the distinction between cyber and physical attack, resulting in offline destruction and physical injury. Moreover, increasing incorporation of augmented and virtual reality technologies into daily life has the potential to result in cybercrimes which entail psychological harm to individuals.

The distinction between legitimate and illegal activity may also become increasingly blurred, since practices such as data harvesting and interception, and reputation manipulation will be even more closely associated with profit generation. Current proximity between criminal spamming and legitimate marketing techniques such as behavioural advertising already serves as an indicator for this. The challenge for legislators will be to delineate the circumstances under which these activities may legitimately be conducted, and to ensure that as far as possible these measures are harmonised internationally. Criminalisation will naturally also require sufficient capacity to investigate, disrupt and prosecute.

Finally, expansion in the use of unmanned vehicles, robotic devices and automation will inevitably raise the issue of whether computers are intelligent agents. This could be a game changer for criminal law, which historically exists to regulate interactions between human beings.

Environmental crime

Environmental crime encompasses a variety of different criminal activities and services various criminal markets. Different forms of environmental crime are expected to evolve significantly over the next years. This is particularly true for the trafficking of e-waste, which is explored in more depth in another chapter of this report.

Stable criminal markets

The EU and its Member States will continue to be threatened not only by the highly dynamic crime areas outlined above, but also by established criminal activities that rely on tried and tested *modi operandi* supporting highly profitable business models. The trafficking in cannabis will continue to generate profits of billions of euros for the criminal networks. Organised property crime will continue to victimise private citizens and businesses over the next decade. The EU will remain a preferred destination for both irregular migrants and traffickers of human beings. The crime areas presented below will remain significant criminal threats to the EU. Established routes, highly developed modi operandi and continuing demand for illicit commodities in the EU and beyond will mean that these criminal markets will persist and continue to challenge law enforcement authorities. These markets represent the largest share of serious and organised crime in the EU currently and will continue to do so in the future.

Cannabis

Cannabis is the most popular drug in EU Member States and is likely to remain so for the foreseeable future. In addition to cultivation in the EU, cannabis is trafficked to the EU in significant quantities from Morocco, Albania and Afghanistan. As law enforcement action becomes more effective in disrupting trafficking activities, there may be significant shifts in the routes used to traffic cannabis to the EU, away from Mediterranean or Western Balkan routes. A decline in trafficking activity is also likely to further reinforce the trend of indoor cannabis cultivation organised by OCGs across the EU. Some Member States with adequate climatic conditions but not previously home to large-scale outdoor production, such as Bulgaria, Romania or Croatia, may become hosts to more significant cannabis production.

It is expected that debates surrounding the legalisation of cannabis are going to intensify over the next ten years, possibly resulting in the legalisation or decriminalisation of the substance in some countries. Any such developments are likely to have a significant impact on the distribution of cannabis within the EU and on the OCGs currently involved in the trafficking and distribution of cannabis. Law enforcement authorities already face widespread social acceptance of cannabis and currently give no reason to expect a significant decrease in the drug's social acceptance in the foreseeable future. The European law enforcement community will need to prepare for potential changes in the legal status of cannabis in parts of the EU.

Facilitation of illegal immigration

Push factors such as armed conflicts, droughts, food shortages and natural disasters will continue to sustain migration flows to the EU from various regions. Countries of origin are set to diversify.

Increasingly, OCGs will focus on enabling long-term stay in the EU by providing advice on how to circumvent or exploit legal systems. OCGs will increasingly rely on modi operandi that are difficult to detect such as marriages of convenience or misuse of other legal statuses. The range of preferred countries of destination in the EU will diversify to include Member States that were previously primarily used for transit.

Some OCGs will develop the capabilities to manipulate or forge chips containing biometric data, such as fingerprints. Alternative modes of transportation such as automated vehicles will be used to travel inconspicuously and without the physical presence of facilitators.

© Shutterstock

Facilitators or intermediaries are regularly exploiting online offers for transportation to arrange intra-EU movements for irregular migrants. Drivers offer rides on popular carpooling websites, which allow drivers to advertise their routes, the number of seats available, and the price per seat. Intermediaries establish contact with the drivers offering ridesharing and arrange for irregular migrants to be transported within the EU. Irregular migrants are regularly intercepted on shared rides on routes such as Hungary – Austria – Germany and Hungary – Austria – Italy – France.

Europol, December 2013

Trafficking in human beings

Trafficking in human beings is one of the oldest criminal activities and will remain a significant source of revenue for OCGs in Europe. The persisting demand for ever-cheaper goods and services, combined with intensified competition between suppliers, drives down prices and creates new opportunities for exploitation. The demand for cheap goods will lead to the increased exploitation of victims on the regular labour market. OCGs will increasingly use legal business structures and sub-contractor arrangements to facilitate illicit employment and exploitation.

OCGs will continue to target vulnerable groups in society for trafficking to Member States with a large market for sexual and labour exploitation. It is conceivable that in the future these OCGs may respond to an increasing demand for the sexual exploitation of European women in countries with emerging middle classes, where European women may be considered 'exotic' and larger profits can be generated for these OCGs.

The use of online services to facilitate the trafficking in human beings will intensify further over the next years. Sexual exploitation using web cams or sex chats emerged together with the proliferation of the internet; future technological innovation will almost certainly give rise to new and previously unknown forms of exploitation.

Organised property crime

OCGs active in organised property crime adapt quickly to changes in their operating environment and continuously look for new opportunities. Thieves may increasingly target electric cars.

Cargo thieves will adapt to this change in logistical arrangements with new modi operandi. Supply chains are likely to become fully automated, with human intervention limited to remote supervision and handling at the origin and destination of transported goods. In response to this development, the theft of cargo may emerge as a profitable cybercrime which relies on intrusion into logistics systems and the diversion of goods to the OCG.

Online platforms will become the main marketplace for stolen goods, largely replacing traditional 'fences', especially for data and

higher value items. Stolen goods are already traded on both the open web and Darknet marketplaces. This development is set to continue and service offerings are likely to become more professional and broader in scope. For instance, rather than having to rely on criminal connections, consumers may be able to buy a stolen car to order, anonymously and with minimal effort. The trafficking of stolen cultural goods is currently a marginal phenomenon. However, as huge markets in China, Brazil and India develop, there may be an unprecedented growth in demand for cultural items, which are seen as status symbols.

Fraud

Ubiquitous connectivity via stationary and mobile devices and a pervasive reliance on online services will drive the evolution of fraud schemes. The widespread exchange of personal information and data between individuals, but also increasingly between citizens and government authorities, is attracting OCGs which are able to generate significant profits from fraud schemes relying on data obtained through theft. OCGs will develop fraud schemes to exploit the increasing delivery of services and education remotely over the internet. The growth of e-commerce is giving rise to a variety of new frauds targeting individual consumers, online vendors and businesses providing money transfer services.

EU and Member State subsidies and other financial incentives are an integral part of many economic policies aimed at stimulating economic recovery and supporting sectors with high- growth potential. OCGs have demonstrated their ability to access and divert public funds, often targeting highly subsidised sectors such as renewable energies. Often relying on the corruption of public servants to facilitate their activities, OCGs will seek to expand their activities to other sectors of the economy wherever opportunities for subsidy fraud appear.

> The "Gameover Zeus"botnet, targeted in May 2014 by a worldwide joint action led by FBI and supported by European Cybercrime Centre (EC3) at Europol is designed to steal banking and other credentials from the computers it infects. Those credentials are then used to initiate or re-direct wire transfers to accounts controlled by criminals. Security researchers estimate that between 500 000 and one million computers worldwide are affected by the last version of the malware that appeared in 2007. Known losses caused by it are estimated around EUR 75 million.
>
> *Europol, May 2014*

Trafficking in firearms

New regions of origin and new OCGs involved in the trafficking of firearms will emerge. A number of conflicts in and near Europe are likely to result in the increased availability of illegal firearms on the international market and their trafficking to the EU across sea and land borders. Some firearms originating from the conflicts in Syria, Libya and Mali are already available on the European black market and these countries may emerge as major sources of illegal firearms trafficked to the EU.

The trade in illegal firearms will increasingly take place online. Technical innovation and greater accessibility have the potential to make platforms and marketplaces hosted on the Darknet significant facilitators for the trade in illicit firearms in the future.

The diversion of firearms from the legal arms trade will remain an important source for firearms trafficking. Despite intense media attention following the presentation of the first 3D printed gun in May 2013, 3D printing technology is unlikely to become a major source for the proliferation of firearms due to the technical complexity of manufacturing functioning firearms using a 3D printer, combined with the ease of access and relatively low prices of firearms traditionally available on the black market in the EU.

Criminal markets in decline?

Criminal markets in decline are expected to diminish over time as commodities change or certain criminal tools become less relevant in a digital age.

Counterfeit currency

Cash will still be needed in the future and will not be replaced entirely by electronic means of payment. The advantages of anonymous money transfers using cash will outweigh the disadvantages. Cash will remain a valuable and stable means of payment, especially in conflict areas, following major natural disasters or in any other situation where infrastructure is not in place to support electronic money transfers.

Criminals will also continue to forge banknotes, which might become polymer based. Polymer-based banknotes will become more sophisticated and able to carry even more complex security features. The raw materials used for currency counterfeiting, such as paper, polymer, inks, and holograms, will become even more widely available. The Darknet will further emerge as a significant facilitator for the trade in raw materials and counterfeit currencies. Digital printers will continue to improve in quality and become more widespread, enabling individuals, not just OCGs, to produce reasonably high-quality fakes.

Cocaine and heroin

NPS which mimic the effect of traditional drugs such as cocaine and heroin may reduce the share of these drugs on European drugs markets. However, cocaine trafficking generates huge profits for the OCGs involved and will continue to do so in the coming years. While it is expected that the number of coca bushes in source countries will decline, genetic modification techniques and new technologies will most likely compensate for this loss through the cultivation of fewer plants producing higher yields. OCGs will continue to diversify their routes and modes of trafficking, exploiting political instability and weak law enforcement capacity in certain regions. The expansion of the Panama Canal will lead to a massive increase in cargo transport, which is of great economic benefit to the EU, but may also create additional opportunities for the trafficking of cocaine.

The Balkan route will remain the most significant entry point into the EU for heroin, even if routes diversify further.

41

© Shutterstock

©Shutterstock

4

THE FUTURE OF LAW
ENFORCEMENT

Delivering law enforcement – challenges and opportunities

Serious and organised crime will remain highly dynamic and quick to exploit changes in the wider environment. Law enforcement authorities across the EU are challenged to keep pace with technological innovation and increasingly complex criminal ventures penetrating all sectors of the economy and society – all the while limiting their expenditure or in many cases coping with shrinking budgets. Mirroring crime, policing is becoming more complex and fighting criminals now requires an unprecedented degree of specialisation and expert knowledge. Law enforcement authorities will have to find ways to reconcile budget constraints with the need for highly specialised knowledge.

Data analytics and Big Data

The proliferation and ubiquity of the internet promises to hold the key to a quantum leap in policing, but also challenges law enforcement to develop the technical solutions, recruit the expertise and make available the financial resources necessary to fully exploit these opportunities.

The rise of Big Data and the emergence of the Internet of Everything will provide invaluable opportunities for law enforcement in developing investigations, identifying and surveilling suspects. Devices such as phones and personal computers currently allow law enforcement to determine the location of an individual. Given the increasing connectivity of products such as clothes, jewellery and footwear, it will become easier to pinpoint the location of a person at a certain time. For example, wearing shoes which automatically connect to the nearest wireless network and post an update to an online fitness profile could allow for a detailed analysis of the movement patterns of an individual. Criminals may think to leave their mobile phone at home, but the increased integration of connective abilities into a wide range of products will make it more difficult to leave no digital trace behind.

Law enforcement authorities will also be able to use Big Data analysis for predictive policing as well as opinion mining. Big Data promises a potential revolution in policing and fighting serious and organised crime. Advanced data analytics can help law enforcement authorities to prioritise their efforts and engage in truly smart and intelligence-led policing. Big Data can reveal patterns in criminal activity and identify links between ostensibly unconnected events or criminal actors directing law enforcement

43

efforts to target the most high-value criminals and to disrupt the work of decentralised criminal networks based online.

However, the potential use of this technology also raises serious questions relating to data protection. Recent disclosures relating to the large-scale interception of personal communications as part of counter-terrorism efforts have revealed that the citizens of many Member States are growing increasingly uneasy about the use of these technologies. Effective law enforcement relies on the trust and cooperation of the public and will need to communicate the nature and limits of Big Data exploitation as part of the work of law enforcement. Effective and reliable data protection as well as transparency are key values that will determine whether law enforcement authorities succeed in retaining the trust of citizens.

Training and recruitment

The use of Big Data and advanced data analytics requires an exceptionally high level of expertise and specialist knowledge that is currently not available to most law enforcement authorities across the EU. Rather than relying on generalist profiles, police officers will need to develop specialisations to carry out complex and specific tasks. The recruitment of specialists will require law enforcement authorities to prioritise and re-assess what law enforcement can deliver and where private sector solutions may be preferable.

Law enforcement authorities are unlikely to be able to compete with the private sector for the most qualified specialists in data analytics in terms of remuneration. Nonetheless, law enforcement authorities will need to find ways to recruit individuals with highly specialised knowledge. It is conceivable that law enforcement authorities will cede some investigative and policing activities to industries. Cybercrime is already largely investigated by private companies working alongside law enforcement. This trend may intensify and find duplication in areas that have not traditionally seen much private sector involvement.

Specialised investigators can already be found in the areas of cybercrime, counterfeiting and financial investigations. As technology progresses and the modi operandi employed by criminal actors become ever more complex, police officers will need to gain specialised knowledge and expertise to counter criminal threats. Technological advances will require the police to employ specialists in fields as diverse as nano-technology and robotics, either as permanent staff or as 'adjunct staff' on retainers.

International and cross-disciplinary cooperation

The globalisation of organised crime has been the topic of debate amongst policy-makers, law enforcement and academia for decades. However, the recognition of this problem has not entailed a globalisation of law enforcement to a degree necessary to effectively counter this threat. International cooperation efforts such as the work of INTERPOL and Europol have been instrumental in highlighting the need and efficiency of international cooperation in fighting serious and organised crime. Criminal actors will soon carry out almost all of their business as part of a virtual and global criminal underworld which knows no borders or jurisdictions. National law enforcement authorities will struggle to disentangle increasingly common criminal structures which operate not only across two or three jurisdictions, but on a truly global scale. International law enforcement cooperation can deliver the tools to counter this threat. However, true cooperation requires the commitment of countries to share data, expertise and resources in order to equip each Member State with the ability to fight new forms of organised crime. International law enforcement agencies such as Europol will remain crucial in building trust between national law enforcement authorities, delivering joint operational capabilities and realising effective international police cooperation.

International cooperation between law enforcement authorities from different countries is a crucial element in the fight against serious and organised crime. The responsibility for fighting

and preventing crime does not solely rest within the domain of law enforcement. The internet has emerged as a highly complex multi-stakeholder environment which is governed largely by private companies rather than state authorities. In the future, law enforcement must engage with the private sector even more than today. Public-private partnerships in fighting cyber-crime are already a reality and there has been some progress in cooperating with companies as brand-holders in the fight against product counterfeiting. However, with an anticipated shift of most organised criminal activity to the virtual realm over the next decades law enforcement must develop inter-disciplinary synergies with partners globally and across sectors.

Private solutions to public problems?

Law enforcement authorities will have to make far-reaching choices, not least on whether to develop capacities within police forces or to outsource these services to providers in the private sector. The private security sector has grown significantly in recent decades. Many functions traditionally carried out by law enforcement authorities are now performed by private security businesses, either as outsourced public functions or as private-sector commercial offerings. Some experts estimate that the private security sector employs more people worldwide than law enforcement. [32] A number of sectors have developed and are further expanding capacities in areas that were previously limited to law enforcement. Banks and insurance companies have their own analysis and investigation units. Private actors, often former police officers, are increasingly offering consultancy services related to these areas. In the past, outsourcing was limited to logistical services, such as cleaning, catering, the maintenance of vehicles, and back-office functions, such human resources and IT. Increasingly, core policing and investigative tasks, including surveillance and patrolling, are carried out by actors outside law enforcement. For years, private investigators have played a major role in criminal investigations relating to fraud and other activities. This development has

led to a situation where traditional 'police tasks' are no longer concentrated within law enforcement authorities and are now carried out by an increasing number of actors in the public and private sectors.

Funding the future

In any future scenario, law enforcement authorities will require funds to invest in new and innovative technologies as well as the specialists who can employ these tools to fight serious and organised crime. Sustained austerity threatens to leave law enforcement behind the curve and unable to close the gap to criminal actors, who continuously innovate and invest. Policy-makers will need to decide on funding models for law enforcement either recommitting a larger budget share to policing or looking at new and innovative ways of funding law enforcement activities and infrastructures.

In the future, some policing services may be delivered through new and innovative forms of collective financing. Crowdsourcing is an emerging business model that has been successful in providing some services and funding for a large number of private ventures. In the future, crowdsourcing among communities may be used to fund policing or the provision of private security. Victims of cybercrime attacks may come together to crowdsource private-sector investigations into cyber attacks, particularly if law enforcement authorities prove unable to investigate an increasing number of incidents. However, this remains controversial on cultural and ideological grounds.

Organised crime is becoming more complex and more diverse and law enforcement agencies will have no choice but to become more flexible and adaptable in their response. Big data and data analytics hold the potential to revolutionise law enforcement approaches to fighting serious and organised crime. However, these developments also represent huge challenges for law enforcement in trying to develop the capabilities to fully make use of their potential.

CONTRIBUTIONS

FROM LEADERS IN LAW ENFORCEMENT, CRIMINAL JUSTICE AND ACADEMIA

Dimitris Avramopoulos,

COMMISSIONER FOR MIGRATION, HOME AFFAIRS AND CITIZENSHIP - EUROPEAN COMMISSION

What is the future of law enforcement in the EU?

What do we know?

Each generation is shaped not only by progressive social and political changes, but also by phenomena that cause suffering, injustice and social disruption. The globalisation of crime, and the effect it has on the lives of each and every citizen, is one of them. The challenge facing us today is to recognise, understand and curb this constantly-changing phenomenon in order to avoid detection.

In Europe today, States are no longer fighting one another by land, sea or air. But there is a new and urgent obligation to fight the traffickers who smuggle people across borders to sell children into prostitution; to intercept ships loaded with drugs that destroy lives; or to take on the challenge of policing cyberspace, where terrorists find new ways to communicate and plan attacks and criminals exploit new markets. Obviously, globalisation has bound Europeans, irreversibly, to even their most far-flung neighbours.

Now, more than ever, there is an urgent need to address organised crime. While the licit economy in the EU suffers one of its roughest patches in decades, the illicit economy is becoming stronger.

Over the last 20 years, organised crime and criminal markets have substantially evolved in the way they operate and broadened their scope to include a modern blend of criminal and licit

activities. Over the last five years, drug trafficking, the main criminal market, has changed. Counterfeit and forged goods are penetrating licit channels of distribution, environmental crime is spreading, smuggling of people is booming. As money laundering, tax fraud and manifold corruption use similar modi operandi, it is increasingly acknowledged that fighting one is combating the others. Finally, as the world relies increasingly on new technologies, it also becomes more cyber-vulnerable.

How have we been mobilising against this threat together? Not well enough. This raises two core questions. What do Member States need from the EU and what does the EU need from the Member States?

Where should we be in 10 years?
A continent-wide fight against these criminal threats, which uses all the legislative and operational tools at its disposal, will be more effective than any national approach. Since organised crime is flexible, opportunistic and resourceful, attempts to combat it must match these qualities. First of all, Member States must strengthen their own resilience and capacity, but given the global nature of security threats, national efforts should be made coherent and fully respect Fundamental Rights. How can this be done?

In ten years, we will certainly have a clearer picture of the geopolitical impact of the illicit economy. By then, the undermining of our legal economies and societies by organised criminal groups will most likely have to be considered as a matter of national and continental security and not just of public security. In such a scenario, the fight against crime and illicit trade would have to be stepped up and mainstreamed through the joint and integrated efforts of governments, law enforcement agencies, diplomacy, defence, regulatory authorities, private sector and civil society via a three-pronged approach; beyond the external borders, at the external borders and within the EU. Needless to say, this approach will have to fully respect the Fundamental Rights of citizens.

Our transnational picture would be significantly enhanced through the development of evidence and intelligence-based assessments and our policies better driven through the combined results of research, stronger evaluation of our actions and improved statistics with a tailored focus on vulnerability, threat and the cross-border dimension. The improved understanding of the relationship between different illicit trades and between illicit

and licit business practices would enhance the resilience of society to crime penetration at local level.

In order to maximise our disruption impact, strategic and operational (risk) analyses would be mainstreamed in the police and judicial work and no longer be confined to money laundering, to the management of external borders or to customs-related fraud. As a result, our actions would be more proactive and targeted by police and judicial officials trained and equipped to address the cross-border dimension.

In the light of transnational threats, information sharing would be viewed as a way of strengthening sovereignty, not surrendering it. Let's face it: even though we are drowning in information we lack specific knowledge. This is where new technologies could help, ensuring both privacy and security, through the interconnection of relevant databases and cross-checking against necessary information held by the private sector. The future of law enforcement will not be about more powers but more expertise in processing available data [33], always with full respect for Fundamental Rights.

Controls at EU points of entry, green and blue borders would be improved through the enhanced cooperation between police, customs and border guards and the development of a genuine EU pre-border intelligence picture, building up on im-proved synergies primarily between Europol and Frontex/Eurosur [34], EMCDDA [35] and MAOC-N [36].

A significant impact on countering threats that the EU is currently facing has been made by the establishment and implementation of the EU Policy Cycle. It is a concerted, intelligence-based approach to fighting priority crime areas in the EU, established by the Member States, with involvement and support by Europol, other EU agencies, the Commission and the Council. The EU Policy Cycle is, as also attested by the current operational successes [37], a consistent intelligence-led approach commonly accepted across the Member States, agencies and international partners, and, most importantly, a clear indication that the multidisciplinary and multi-agency approach works and produces significant concrete operational results.

Together, let's shape the future of law enforcement, on the basis of our founding values of fair cooperation and solidarity.

Les hommes n'acceptent le changement que dans la nécessité et ils ne voient la nécessité que dans la crise.

Jean Monnet

© Shutterstock

Jörg Ziercke,

FORMER PRESIDENT - FEDERAL CRIMINAL
POLICE OFFICE/BKA, GERMANY

Suppression of organised crime in the digital age

The digital age is increasingly shaping national and global economic agendas as well as the private and professional lives of each and every one of us. Worldwide connectivity and global digitalisation are only two aspects of this.

The internet is an integral part of the digital age and today's global world. At the same time, it is a significant component of modern crime. A digital revolution in communications technologies and nearly global freedom of movement have contributed considerably to the diminishing relevance of borders for criminals active on a global level. The activities of organised crime are no longer restricted to a specific geographical area. Organised crime has become truly transnational.

An estimated 3 600 criminal groups are active in the EU. These groups are increasingly flexible, innovative and global in outlook and do not confine themselves to committing one type of crime. They are quick to adapt to technological advances and adopt them as part of new modi operandi.

Until now, law enforcement tended to focus on traditional organised crime phenomena such as Italian mafia organisations, drug cartels or outlaw motorcycle gangs. However, in future, we also need to look more closely at new or evolving forms of organised crime such as cybercrime and economic crime. At the same time we need to keep a close eye on so-called mass crimes in the areas of fraud and property crime. Wherever there is money to be made, organised crime will attempt to gain a foothold; the quicker and more, the better. From a phenomenological point of view, a significant transformation has taken place in recent years. Law enforcement authorities throughout the world are increasingly confronted with cybercrime. The threats emanating from the diverse facets of cybercrime will continue to increase in their magnitude and diversity. However, this does not necessarily mean that traditional types of organised crime, such as drug crime, will decline in importance as criminal threats. This trend will continue and become more pronounced in the years to come.

Such phenomenological transformations mean that investigations will be confronted with new challenges. The increasing professionalism displayed by these groups, especially with regard to the use of modern means of communication, the large proportion of internationally operating groups of offenders and the mobility of OCG members place heavy demands on law enforcement and prosecution authorities both at home and abroad.

For the EU, this means that Member States have to cooperate even more closely in the area of law enforcement and that the European security architecture has to be developed further. As part of this process, Europol at a police level and Eurojust at a judicial level have key roles to play as the leading agencies in the fight against crime in the EU.

Parallel to such organisational adjustments, which have already been initiated, the process of judicial harmonisation within the European Union must be expedited with due regard given to national particularities. This means that in addition to establishing a uniform understanding and an EU definition of organised crime, we must also adapt substantive criminal laws in the area of serious and organised crime.

Useful instruments already in use, such as joint investigation teams, must and will become standards for a multinational suppression of cross-border organised criminal groups.

Another joint European measure within this context is the establishment and implementation of uniform training standards in all the Member States. The aim here is to recruit skilled personnel (especially in fields which require technical expertise) so that we can respond even quicker to technological changes and advances used to commit crimes.

In spite of all the negative influences the digital age has had on the development of serious and organised crime, the opportunities afforded by the global exchange of information 'just-in-time' have provided law enforcement authorities with communication possibilities for effective and global law enforcement undreamt of just a few years ago. We must extend the scope of these digital possibilities and use them more intensively. The fight against organised crime in the digital age poses a major challenge not only to national and international law enforcement authorities, but to society as a whole. Cooperation with all the relevant forces is required if we are to fight organised crime in an effective and lasting way within the framework of the European security architecture. This applies to measures in the field of law enforcement or threat prevention, regulatory provisions or forms of co-operation with partners in the private sector, research and relevant non-governmental organisations.

> *Member States have to cooperate even more closely in the area of law enforcement and the European security architecture has to be developed further.*

Glyn Lewis,

DIRECTOR SPECIALISED CRIME AND
ANALYSIS - INTERPOL

Collaboration for bringing about a safer world needs to go beyond traditional frameworks that bind law enforcement and international police cooperation.

An outlook on global law enforcement cooperation over the next 10 years

One hundred years ago, at the first International Criminal Police Congress held in Monaco, police officers and judicial representatives from 24 countries discussed ways to cooperate better on solving crimes. Participants at the Congress expressed 12 wishes for the future of international police cooperation, for example direct contact points in national police forces; the need for fast international police communications; common languages; training; improved identification systems; centralised and standardised police records; and streamlined extradition procedures. It was also the triggering event for founding INTERPOL in 1923.

Looking at the principal concepts and needs for international policing at that time we see that most of them are still valid and they are at the heart of INTERPOL's work today. But they will even be more and more important in future, in particular as the challenges have evolved and will do in the future.

The world is becoming more global and interconnected. With the intention for deeper economic integration, national borders are abolished to increase the circulation of people, goods, money and services. For instance, the gradual regionalisation of borders, for example within Western Africa and Southeast Asia, creates new opportunities, but on the other hand makes it difficult for police to control the flows which are also exploited by international criminals.

But not only the physical world becomes more and more interconnected, also the virtual world. New trends in cybercrime are emerging all the time, with costs to the global economy running to billions of dollars. Criminal organisations work with criminally minded technology professionals to commit cybercrime, often to fund other illegal activities. The increasing emphasis on networks leads to a rising role and number of interconnections with a great risk potential for rapid disruption. The extension and deepening of networked infrastructure raises the concomitant risk of greater collateral damage caused by disruptions to single nodes within the networks. Cyber-attacks on critical infrastructure are the most infamous examples of this. Future threats could be smaller, less detectable and much faster than before; where assailants could not be only backed by outfits or organisations, but act as 'lone wolves'; where potential targets could multiply exponentially. In future society will face an expanded vulnerability.

But next to these evolving challenges police worldwide are confronted and will be confronted with far-reaching effects of fiscal austerity for many police forces. Policing budgets will be affected, with possible cuts to operational and organisational budgets, and stricter measures of performances tied to future budgetary allocations.

Enhanced international policing needs to become the flipside of this increased interconnectivity both in the physical and virtual world. We need a better information exchange with secure communication channels globally and beyond the different regions as criminals also work across the globe. At the heart of this increased information exchange we need to make the information available at the right time to the right recipients, providing instant access to criminal data by establishing and maintaining databases at regional level and global level.

Looking at the financial and resource constraints of police worldwide, we have to improve our cooperation, coordinate and plan our work in a better and more complementary way to avoid overlaps and double work. Although now and in future regional police cooperation gets more structured and organised with regional cooperation mechanisms and bodies established, there is a need for a global and integrated approach, linking the different regions of the world. Here it is important to avoid working in silos and make information systems interoperable and connected. Collaboration for bringing about a safer world needs to go beyond traditional frameworks that bind law enforcement and international police cooperation. Partnerships beyond law enforcement are critical to deal with emerging threats and challenges. In today's world, innovation resides in the extensive research and development fostered with the private sector. We must work together in forging alliances to pool our resources and reach our shared goals and do so while also remaining impartial.

Then only together we can build a safer world.

Catherine De Bolle,

COMMISSIONER GENERAL - FEDERAL POLICE, BELGIUM

I am grateful for the opportunity to contribute to this Europol report. I have written this contribution in my capacity as the Commissioner General of the Belgian Federal Police advocating real and tangible progress in the organisation of operational police cooperation in the EU.

Let me start by stating the obvious. European police cooperation will remain an absolute necessity and even increase in importance. Budgetary restraints will affect law enforcement authorities at least until 2020. These measures make effective operational cooperation among Member States in fighting serious and organised crime a mandatory requirement. At the time of writing this contribution, the Operational Action Plans for 2015 within the EU policy cycle on serious and organised crime and the next EU Internal Security Strategy are being developed. Although I fully support those instruments, they are only a general starting point for operational police cooperation and extra effort will still be required from Member States and EU agencies to transform these into operational reality.

It is my personal observation that, too often, there is still reluctance among Member States to exchange information. In some cases, this affects how we describe certain criminal groups, identify specific threats or confront difficulties in organising ourselves on a national level. If we want to progress, we need to abandon these reservations. We need to try to mature as a family of Member States and be more open and frank with each other.

We need to realise that we cannot expect the EU to take on all of our individual criminal threats and priorities at the same time. This particularly highlights the importance of a methodological and planned approach such as the EU policy cycle. I am absolutely convinced that this is the right way to tackle serious and organised crime operating on an international level. However, the policy cycle needs to focus even more on tangible operational action. I sincerely hope that, if all Member States and

agencies commit to this, we will end up with evaluation reports showing the number of arrests and criminal groups disrupted instead of reports calling for more operational actions and the appointment of drivers with the right profiles.

Furthermore, real progress needs to be made in developing an external security strategy which takes into account internal security threats. Internal security aspects should be an important part of EU missions and taking these into account in negotiations for cooperation arrangements with third countries is an absolute necessity. A clear example of this is the problem of foreign fighters which will require us to cooperate with countries neighbouring Syria and Iraq.

We can still do more to improve the exchange of information between Member States and EU agencies after all these years.

I am convinced that international cooperation should not be restricted to a central national level and that – where possible – it is our responsibility to connect much more on decentralised levels in order to get the right information to the right place. For non-common law countries, a closer relationship with the judiciary at national level will also be crucial, as the judiciary often determines the scope of the investigation. I am aware that this is not something that can be easily achieved, as it will require efforts in each Member State on organisational, technical and functional levels. In Belgium, we have recently taken first steps for such an approach.

Technological advances hold significant opportunities for the more efficient and effective

51

exchange of information. On the EU level, initiatives to take advantage of these advances are already being developed such as the much needed interoperability project which aims at enhancing cooperation with Interpol and Europol. The success of the Secure Information Exchange Network Application (SIENA) proves that a well-functioning tool quickly improves information flows and generates ideas for further development. Financial support provided by the European Commission is required in order to integrate these and other similar projects into national information exchange environments.

At the same time, we as police need to respect data protection and human rights legislation. I remain strongly convinced that this aspect of law enforcement work is a fundamental necessity. However, recent developments on national and EU levels indicate that it is likely to become more difficult to strike the right balance between respecting those principles and the need to share information among police forces. As part of a case due to be considered by the Belgian Constitutional Court, the Belgian League of Human Rights is set to argue that the international exchange of personal information should only be possible if the concerned person has already been found guilty. Considerable effort in communicating with data protection and human rights bodies both nationally and internationally will become an even more important aspect of our work.

In closing, I would like to shortly address the future of Europol. Broadly speaking, the ambition for Europol to become "a hub for information exchange between the law enforcement authorities of the Member States, a service provider and a platform for law enforcement services" will remain unchanged. It is my belief that Europol's core activities will need to be centred even more on its analytical capacities, both for strategic analysis and especially operational analysis. Together with the Member States, Europol will need to further define how information is shared with Europol and what Member States can expect from Europol as added value. In this regard, I expect a transparent and open debate in order for Europol to develop the "integrated data management concept" as a modern future-proof concept.

Keith Bristow,

DIRECTOR GENERAL – NATIONAL CRIME AGENCY, UNITED KINGDOM

The future: challenges and opportunities for Law Enforcement

Emerging and Future Threats

The scale and pace of change in criminality that law enforcement faces today should not be underestimated. We live in an increasingly digital age, where new threats will continue to emerge from new sources and traditional crimes will continue but also adapt in line with new technology:

- Data and data management services are developing rapidly, providing increased opportunities for criminals committing both cyber dependent and cyber enabled crimes;

- The use of encrypted/anonymous communications is likely to increase amongst criminal groups, including, for example, those creating and sharing indecent images of children;

- A key theme in the UK's National Strategic Assessment (NSA) 2014 is the anticipated growth in the targeted compromise by cyber criminals of UK networked systems, including more ransomware, distributed denial of service (DDOS) and Malware attacks; the latter being a high priority threat in the UK's National Control Strategy as an enabler to commit fraud offences against individuals and organisations.

Delivering the Law Enforcement Response of the Future

In line with these emerging threats, law enforcement needs to be innovative and agile in its response. We need to do more than just 'keep up' with these changes: we must identify and respond to future threats and opportunities before they even occur. At the same time law enforcement needs to continue to build public trust and confidence so that it can continue to be able to use key capabilities.

To meet the needs of the future, in April 2014 the NCA established Novo, a five year change programme which is helping the NCA to make radical and positive changes in the development of its capabilities, work practices, culture and infrastructure.

The NCA's National Cyber Crime Unit (NCCU), which leads UK law enforcement efforts to cut serious and organised hi-tech crime, is also recruiting new officers for roles across a range of computer science disciplines, including software development, network engineering, digital forensics and online investigation.

Investment in technology and in specialist skills will provide more effective tools for investigations and potentially enable significant future savings and efficiencies but these will require initial investment that will be challenging though vital to deliver in straitened times.

The rewards for doing the hard, right thing in terms of future investment will be opportunities to have a profound disruptive impact on new and emerging crimes. Advanced criminal intelligence gathering will be the norm. Further, investment in systems to extract, link, analyse and interpret data will enable us to streamline operations and enable better decision making.

Equally important, the law enforcement response to serious and organised crime must be one of domestic and international collaboration, including public and private sector partnerships. Two current NCA cyber investigations inform a common understanding of how this can work:

Operation TOVAR is an investigation focusing on the 'GameOverZeus' and 'CryptoLocker' Malware variants, estimated to have cost the UK £500 million in losses. In June 2014, the NCA coordinated activity with international law enforcement including: the

European Cybercrime Centre based in Europol; industry partners; and GCHQ, to take the botnet underpinning these attacks offline for two weeks.

Impact: A media campaign advised the public to update their computer operating systems and antivirus protection, and to clean their computers of any Malware. This led to a marked increase in downloads of Malware removal tools, a significant drop in breaches attributable to this botnet, and a comparable drop in losses suffered by the financial sector. Data from industry partners suggests that since the activity there has been a 32% decrease in total UK GameOverZeus infections;

Project DISPUTED is an NCA-led investigation which targets the Shylock Malware variant, a sophisticated system employed by criminals to steal online banking credentials, targeting the UK banking sector in particular. Shylock has infected at least 30,000 computers running Microsoft Windows worldwide. Intelligence suggests that Shylock has to date targeted the UK more than any other country, although the suspected developers are based elsewhere.

Achievements: In the first project of its kind for a UK law enforcement agency, the NCA brought together partners from across law enforcement and private sectors, including Europol, the FBI, BAE Systems Applied Intelligence, GCHQ, Dell SecureWorks, Kaspersky Lab and the German Federal Police (BKA) to jointly address the Shylock trojan. As part of this ongoing activity, law enforcement agencies are taking action to disrupt the infrastructure which Shylock depends upon in order to operate effectively. This has been conducted from the operational centre at the European Cybercrime Centre in Europol.

These investigations provide an indication of what can already be achieved through a collaborative, agile and innovative law enforcement led approach. With further collaboration, and investment in technology and specialist expertise in the present, we can collectively ensure we are fully able to identify, anticipate and address the serious and organised crime threat in the coming years.

Ints Kuzis,

CHIEF OF THE STATE POLICE - LATVIAN STATE POLICE, LATVIA

The Latvian presidency of the Council of the European Union (EU) commenced on 1 January 2015. The tasks of Latvia during the presidency are mainly defined in the 18 month programme (1 July 2014 – 31 December 2015) of the Council prepared by the trio presidencies of Italy, Latvia and Luxembourg. These priorities clearly set out the importance of implementing the strategic guidelines for legislative and operational planning for the coming years within the Area of Freedom, Security and Justice [39] and were confirmed by the European Council on 26th and 27th June.

The fight against crime and terrorism as well as the fight against corruption and radicalisation while guaranteeing the protection of balanced fundamental rights, including personal data, are key tasks in the area of internal security.

The Latvian State Police will carry on the work already achieved in the area of internal security by strengthening cooperation and participating in the discussion on an update of the EU's Internal Security Strategy.

Strengthening the fight against organised crime is a key priority and requires balanced coordination and management. Latvia will continue participating in the development of the legal framework governing law enforcement cooperation in the EU and will work with other Member States to further improve the work of the European Police Office (Europol) and the European Police College (CEPOL). We consider the passenger data register an important tool in the fight against serious crime and terrorism.

Five strategic objectives will serve as the basis for an update of the EU's Internal Security Strategy:

1. disruption of international criminal networks;

2. prevention of terrorism, including radicalisation and recruitment for terrorism purposes;

3. raising levels of security for citizens and businesses in the cyberspace;

4. strengthening security through border management;

5. increasing Europe's resilience to crises and disasters.

The EU policy cycle on serious and organised crime will continue to coordinate operational cooperation on the nine EU priorities for the fight against serious and organised crime for 2014-2017 [40], adopted by Council of Justice and Home Affairs Ministers and supported by Latvia. The policy cycle not only considers existing priorities but also takes into account new possible threats, as well as any activities related to money laundering, criminal infiltration into the legal economy, corruption in order to acquire assets and to seize the proceeds from crime. In this regard, Latvia emphasises that the effective fight against organised crime depends on an integrated approach bringing together all relevant parties involved at the level of the EU Member States and the EU.

The European Multidisciplinary Platform against Criminal Threats (EMPACT) is crucial in strengthening cooperation between competent authorities. Latvia sees a need to raise the level of awareness and understanding of the policy cycle and its priorities in the Member States in order to facilitate more active involvement of experts from the Member States in implementing the EU priorities, efficiently and purposefully combining priorities defined at the EU level with measures at the national level.

We hope that Europol's Interim Serious and Organised Crime Threat Assessment (SOCTA) 2015 will define existing and emerging criminal threats to the EU and its Member States. On the basis of the Interim SOCTA, the relevance and development of the existing EU policy cycle priorities for the fight against organised crime for 2014-2017 will be reviewed and potential new threats in the area of serious and organised crime will be assessed. Further improvements to the SOCTA Methodology will

© Shutterstock

ensure more added value and increased quality of the SOCTA.

The Latvian State Police considers joint operations of Member State law enforcement authorities an effective cooperation mechanism. This has been proven by Operation Archimedes, which took place in September 2014. Europol is in an ideal position to co-ordinate such measures. Further targeted operational measures will require EU financing in order to further enhance the cooperation between the Member States.

The Latvian State Police monitors new and emerging threats and will continue to pay special attention to improving capabilities for the fight against cybercrime. This type of crime is an increasing threat for the EU and supports criminal groups conducting various other criminal activities. The Latvian State Police emphasises the necessity to protect children in digital environments in particular, to prevent the production and distribution of child exploitation material and other forms of sexual abuse online.

Latvia is committed to enhancing the implementation of the Strategy Towards the Prevention and Eradication of Trafficking in Human Beings [41], paying special attention to particular threats such as illegal employment and sham marriages.

Latvia foresees the implementation of the 2013-2020 EU Drugs Strategy and the 2013-2016 EU Drugs Action Plan. The Latvian State Police pays special attention to the necessity to improve legislation controlling new psychoactive substances and calls for an effective instrument in the fight against this increasing threat.

The Latvian State Police is ready to contribute to the fight against serious and organised crime and will mobilise its forces within the limits of its capacity and financial resources. The Latvian State Police will take measures to achieve the objectives and realise the tasks defined as part of the EU's shared priorities in the Area of Freedom, Security and Justice.

The European Multidisciplinary Platform against Criminal Threats (EMPACT) is crucial in strengthening cooperation between competent authorities.

55

Alessandro Pansa,

CHIEF OF POLICE – DEPARTMENT OF PUBLIC SECURITY, ITALY

The process of building a secure Europe, able to increase its prospects for development, necessarily requires the constant fight against all forms of crime threatening the daily lives of its citizens. This objective, as part of a wider strategic vision, can only be achieved through appropriate system synergies involving all the institutional actors entrusted with the fulfilment of this goal.

In this context, the European law enforcement services will need to assume an increasingly significant role using an approach that takes into account the evolution of criminal phenomena and enables the consequent adjustment of operational responses.

The transnational dimension of the most worrying criminal threats is facilitated by the weakening of borders between the Member States and by the adaptability of major criminal groups, which are able to find new forms of organisation in a "globalisation" context.

The experience we have gained in countering criminal threats over the past years will enable us to anticipate emerging threats from serious and organised crime and allow us to take measures to fully realise a European Area of Freedom, Security and Justice. A careful analysis of the results in the fight against organised crime already achieved will allow us to draw a coherent map of the organised crime landscape in Europe and identify areas where law enforcement efforts should be focused.

The threat represented by religiously motivated terrorism is, perhaps, the context in which our organisations will have to demonstrate the ability to renew their analytical skills in order to prepare an adequate response in terms of prevention and fight. The synergies between all the European stakeholders in the field of security will facilitate the creation of shared strategies to address the danger posed by the less structured forms of Islamic terrorism.

The integration of the various databases and the development of better systems for the collection of the data regarding the movements of potentially dangerous "travellers" at European level will be fundamental tools for the early detection of terrorists in the near future. At the same time, law enforcement responses to these threats can be enhanced by adopting more flexible operational models such as "multilateral ad hoc teams" and common training paths that facilitate the understanding of the various linguistic and socio-cultural connotations of the phenomenon.

Over the next years, law enforcement services will be increasingly committed to stemming illegal immigration into the EU. An effective strategy in this field will require the participation of all the countries involved in the management of migration flows. It will be necessary to find a balance between the requirements in the fight against the criminal organisations exploiting migrants and the protection of victims' fundamental rights through the sharing of objectives between the partners involved. EU agencies like Frontex and Europol will have a fundamental role in ensuring the effective protection of the common European borders and are crucial in enabling Member States to quickly respond to the rapid evolution and increasing scope of various criminal phenomena over the years.

Over time, the concern for security will increasingly shift its focus towards the protection of computer environments. Cyberspace is the environment where criminals will test their capacity for innovation, endangering particularly sensitive legal interests. The exposure of financial transactions on the Internet to cybercriminals and the dangers posed by the anonymity offered to criminals are already significant threats.

In this field, a primary objective will be to continue on the path of research and education, including through targeted partnerships with the private sector. This approach will enable us to significantly reduce the vulnerabilities linked to web access.

In conclusion, during the second decade of the new millennium, the mission of law enforcement will be even more complex considering the speed with which serious crime evolves. The sharing of "best practices" and training as well as the circulation of real-time information, which is fundamental to effective police cooperation, will be the most important instruments in enabling us to meet future challenges.

Michèle Coninsx,

PRESIDENT - EUROJUST

The JHA agencies within their respective mandates and the national judicial and law enforcement authorities in the Member States must continue promoting close cooperation in the decade ahead to protect European citizens against new threats affecting the security of the European Union. The European Council has called for an enhanced role of the JHA agencies within the development of a true Area of Justice, Freedom and Security.

To effectively prevent and fight serious cross-border crime and terrorism a multidisciplinary approach is highly recommended. An approach that integrates criminal and security policies, that incorporates investigations and prosecutions as complementary to administrative/executive measures, and is a necessary consequence and measurable outcome of information exchange and tactical (police) actions. It also requires the collaboration and active involvement, as appropriate, with other stakeholders, which might include administrative authorities, other EU agencies and EU networks, private stakeholders and non- profit organisations, and is crucial to developing partnerships in innovation and ensuring that technological developments are advantageous to national competent authorities rather than criminal networks and organisations.

In fraud and money laundering cases (highest number of case referrals), Eurojust plays an important role by promoting the involvement of administrative authorities in criminal cases and, where possible, the participation of authorities such as customs and tax authorities, in coordination meetings and JITs. [42] The information and documentation that can be retrieved from public administration is valuable for presenting solid expert reports in court as evidence. [43] Considering the new Directive on the prevention of the use of the financial systems for the purpose of money laundering and terrorism financing, [44] closer collaboration with the European Banking Authority will most likely contribute to the detection of criminal activities involving money laundering. Other examples of collaboration are the commitment of private companies to fighting child pornography (within the framework of the European Financial Coalition against sexual exploitation of children online) and to the detection of terrorist plots and the tracing of the perpetrators (within the framework of Passenger Name Records and Terrorist Finance Tracking Programme agreements with the United States). Further possibilities of this kind of collaboration must be explored, for example, with the International Criminal Court and the EU's genocide network [45] with regard to crimes of genocide, crimes against humanity and war crimes.

To effectively prevent and fight serious cross-border crime and terrorism a multidisciplinary approach is highly recommended.

In the current context of increasing globalisation and geopolitical instability, with emerging forms of criminality, legislative initiatives and criminal policies are needed regarding the prevention of radicalisation and extremism, actions against aspiring foreign fighters and returnees and passive training in terrorism (currently not covered by national legislation).

Cross-border crime and, increasingly, crimes without clear borders such as cybercrime, present a particular challenge due to the involvement of different jurisdictions and are therefore an additional hindrance for the prosecution to determine the competent authorities. Legal obstacles to judicial cooperation in criminal matters remain a challenge. Consistently transposing and effectively implementing key existing legal measures and policies, mutual recognition instruments and newly developed instruments (e.g. the Directive on freezing and confiscation and the Directive on the European Investigation Order), are needed to ensure the prosecution and conviction of perpetrators, particularly through the freezing and confiscation of the proceeds of crime, making the effective dismantling of criminal networks feasible. Among the rules applicable, those regulating the fundamental rights of suspected and accused persons are crucial. The adoption and implementation of relevant legal provisions on the protection of the rights of victims of crime and the procedural safeguards for the suspects or accused must be ensured. [46]

Provisions and time limits on data retention, the identification of the competent jurisdiction (including in cases of conflicts of jurisdiction), the different rules on gathering, admissibility and disclosure of evidence, and differences in substantive and procedural laws, can affect judicial cooperation. Eurojust will continue to contribute to improving judicial cooperation and mutual trust, also with third States, by building bridges between the different judicial systems. Effective and efficient support for the competent national authorities calls for closer operational cooperation and partnership between EU partners, based on an effective information exchange and complementarity.

In this context the strengthening of mutual trust between law enforcement and judicial authorities is essential. Eurojust's coordination meetings allow for law enforcement and judicial authorities to complement each other in developing common investigative and prosecutorial strategies (e.g. issuing and executing European Arrest Warrants; simultaneous arrests and searches; controlled deliveries), with the support of Europol and involved third States. Joint investigation teams have also proven to be very effective, obliging law enforcement and judicial authorities to work together in ensuring that the information and evidence collected will be admissible and properly assessed in court. Last but not least are the coordination centres established at Eurojust providing real-time support during action days by facilitating decision making and immediate responses.

Eurojust has managed various strategic projects [47], such as in the area of trafficking in human beings and drug trafficking, organised thematic seminars to bring together practitioners and involved actors, such as the Prosecutors General, to exchange experience and best practice and consequently produced reports and other products, such as the Terrorism Convictions Monitor. These activities remain necessary, as well as training, the latter being a permanent challenge for prosecutors and judges.

The European Public Prosecutor's Office (EPPO), as a future new EU actor in the fight against crimes affecting the financial interests of the European Union, will profit from Eurojust's operational experience in international judicial cooperation and the tools it has developed to succeed in its operational work.

Partnership and synergies between EU actors are indispensable. In the next 10 years, Eurojust will continue to promote close cooperation with all the partners concerned.
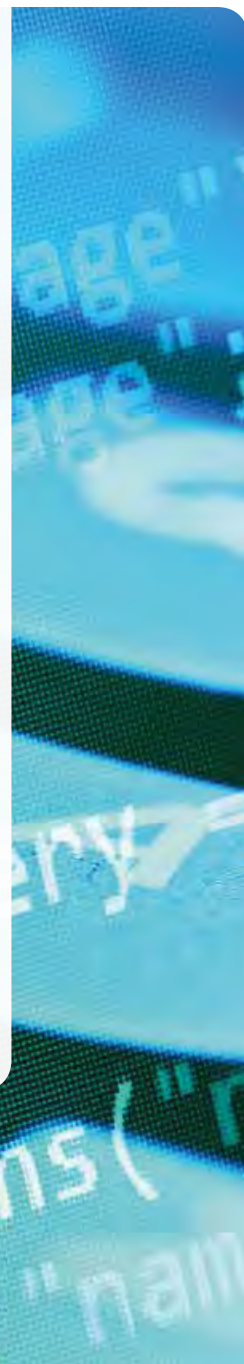
The SOCTA Academic Advisory Group (from left to right):

Prof. Max Taylor, Prof. Michael Levi, Dr Xavier Raufer, Prof. Ernesto Savona, Prof. Dr Arndt Sinn, Prof. Alain Bauer (not in picture)

Contribution from the SOCTA Academic Advisory Group

The Academic Advisory Group was pleased to be invited to participate with Europol staff in developing and commenting on the report 'Exploring tomorrow's organised crime'. We recognise and appreciate the innovative partnership that Europol has developed through engagement with experts outside of the police service in the preparation of a report of this kind, and we would at the outset like to congratulate the Europol staff on the production of a challenging and well-documented report. This Report will provide European law enforcement authorities, policy-makers and legislators with important comparative benchmarks as an aid in future planning.

We welcome the systematic forward-looking qualities of the Report, and in particular note the significance of identifying a series of key drivers for change.

We will structure our comments under two broad headings:

• Reflections on the report;

• Further commentary identifying issues that we feel may be important in identifying future trends.

Reflections on the Report content.

1) We welcome the systematic forward-looking qualities of the Report, and in particular note the significance of identifying a series of key drivers for change.

2) Predicting future developments is always difficult and challenging. Future predictions of crime based on actuarial and probabilistic methodologies, may appear to have a numerical, and therefore scientific validity. Unfortunately they are generally flawed as reliable predictors of innovation, as opposed to the repetitive qualities of much criminal behaviour. It is innovation

59

> *It is innovation in criminality, however, often driven by external forces rather than a continuation of the present, that produces the greatest challenges for law enforcement.*

in criminality, however, often driven by external forces rather than a continuation of the present, that produces the greatest challenges for law enforcement. Developments in digital technologies in particular have challenged the capacity to forecast and battle future crime trends. There is every indication that the pace of innovation in this area will increase. Law enforcement responses to this have not only to address criminal behaviour, but also need to maintain the balance between security and freedom. Maintaining this balance represents a fundamental challenge in the face of the current adaptive, innovative and fluid crime landscape. We believe that balance can be best maintained when good law enforcement practice is informed by sophisticated analysis to inform policy decisions. But in this context, over-bureaucratised government, slow analysis and responses, and inflexible administrative frameworks will offer opportunities for criminal networks to exploit, especially in a context driven by rapidly evolving technologies of communication and payments systems. Law Enforcement and the administrative environment in which law enforcement organisations work will need to be dynamic, flexible and responsive to address these future challenges.

3) The report addresses the question of a new definition of organised crime. We consider the challenges that future developments may present to how we conceptualise organised crime to be a matter of great importance, but we would urge caution. Any new or modified definitions need to be firmly evidentially based, and need to be viewed from both a national and European (and beyond) perspective. Common research is the key to find the new faces of organized crime.

Further Commentary

1) We believe our added value to this process is highlighting and emphasizing what we see as significant future trends. What follows has its origins in this Report, and in the previous Europol SOCTA 2013.

2) As a general point, we expect existing crime types to continue, but to be supplemented with economic crime opportunities available to offenders located anywhere in the globe, particularly boosted by the Internet. Thus, European initiatives will have to be framed within a broader context of global common legislative provision – however uneven - where currently practical cooperation and resources do not always reflect legislation. In the 1970s, early criminal activities using computer-based technology were examined by criminologists and futurologists. Even then, it was apparent that the incidence of such crimes would grow, and subsequently we have seen in recent times massive frauds that have caused major financial losses to banks, credit card holders and major retail corporations. The process was probably slower than anticipated, but has been much deeper. Addressing this will represent a major challenge to European Law Enforcement Organizations, but significant resources will need to be deployed to improved co-operation and common responses, and this will be a challenge to traditionalists in Member States.

3) Some future crime trends are already apparent – the changes in different forms of drug usage and their production, the enormous growth in counterfeit goods, the changing nature of terrorist activity (in particular the diminishing incidence of attacks, the changed nature of terrorist engagement and the growth of hybrid terrorism – part ordinary criminal, part terrorist), and the changes in financial offending and criminal exchange influenced by digital technologies. To stay abreast of these changes, Law Enforcement agencies will need to adopt innovative approaches to crime management,

drawing on both civil society structures and commercial organizations as partners. Partial externalization of law enforcement provision may be an element of this, which may present particular national difficulties of application and two-way information exchange. But the current trend for Law Enforcement to engage as partners with external experts to provide expertise and enhanced capacity will undoubtedly grow in importance. This will require careful and perhaps challenging administrative provision and governance. An investment in planning for this at a European level needs to be a high priority.

4) Specifically, we might note that crime trends are a function of motivations, opportunities and the way both public and private sectors intentionally or accidentally intervene to collect intelligence and act against opportunities. Long term trends include the ways in which technology impacts to industrialise opportunities (for example enabling the purchase of easy-to-use e-crime kits and identity fraud data that lower the entry level into crime; enable financial transfers via Bitcoin-like anonymising vehicles in which criminals can plausibly trust). Market-based offences like drugs and people smuggling and vice will still provide cash based and non-cash opportunities for those with the networks and varied organisational skills to take advantage. It would therefore be wrong to expect in the future traditional 'criminal types' to be eliminated from the market by developments in communication and e-commerce.

5) There may however be more scope for 'organised crime networks' to use electronic means to insulate themselves from risk and widen their financial crime activities. There may also be greater scope to entrap insiders in banks and other institutions to provide financial information and money laundering services, subject to counter-measures from compliance officers to track those risks. This is a challenge for law enforcement and intelligence officers to collate and respond to these evolving approaches, and

to continue to broaden their intelligence sources and intervention efforts away from drugs networks to these other spheres.

6) A particular potential future challenge that can be identified may be the growing significance for criminal behaviour of distributed non-hierarchical networking expressed as complex global conspiracies. These are currently most evident in Internet related arenas, and they challenge our understanding of the relationship between online and offline offending. Traditional hierarchical networks are already of diminishing significance in terrorist organisations, and there is good evidence of their diminishing significance in criminal activity. Social networking, and the 'dark web' already make such complex 'flat' networks a reality in Internet based offending, and the influence of this is likely to grow. These trends will present both conceptual and organisational challenges for law enforcement. It requires a rethinking of the idea of an 'organised' structure, and monitoring and surveilling such networks are extremely difficult.

7) In order to respond to the indirect and unintended effects of their own production and marketing behaviour, private sector organisations may have to develop enhanced forms of regulation and policing. In some measure this already happens, but the management, integration with public provision and control of such activities will challenge administrative and law enforcement provision. Furthermore, the spread in the concept of public safety to include food security and similar issues will present many challenges for Europol and other policing bodies who will need to intersect with broader commercial issues to address these problems, in ways that they have not commonly had to deal with in the past.

8) Information collection and sharing has greatly improved within Europe. But analysis is at times weak, which suggests a need for greater investment in analytical capabilities.

© Shutterstock

61

Endnotes

1. OECD, Strategic Transport Infrastructure Needs to 2030: Main Findings, 2011, accessible at http://www.oecd.org/futures/infra-structureto2030/49094448.pdf

2. FIDIS Deliverable 3.10 Biometrics in Identity Management [online] Available at: http://www.fidis.net/resources/fidis-deliverables/hightechid/int-d37001/

3. EU Scientific Committee on Emerging and Newly Identified Health Risks, The appropriateness of existing methodologies to assess the potential risks associated with engineered and adventitious products of nanotechnologies, 2006.

4. European Commission, Preparing for our future: Developing a common strategy for key enabling technologies in the EU, 2009

5. United Nations Interregional Crime and Justice Research Institute, Security Implication of Synthetic Biology and Nanobiotechnology, 2012

6. European Commission, Information and communication technologies: Work programme 2013, 2013

7. BBC News, "Is e-waste an untapped treasure?", 19 February 2014, accessible at http://www.bbc.com/future/story/20140218-why-your-old-tech-holds-treasure

8. Environmental Leader, "E-Waste to Exceed 93.5 Million Tons Annually", 24 February 2014, accessible at http://www.environmentalleader.com/2014/02/24/e-waste-to-exceed-93-5-million-tons-annually/

9. BBC News, "Is e-waste an untapped treasure?", 19 February 2014, accessible at http://www.bbc.com/future/story/20140218-why-your-old-tech-holds-treasure

10. Environmental Leader, "E-Waste to Exceed 93.5 Million Tons Annually", 24 February 2014, accessible at http://www.environmentalleader.com/2014/02/24/e-waste-to-exceed-93-5-million-tons-annually/

11. The Huffington Post, "How Do You Recycle a Solar Panel?", 23 January 2014, accessible at http://www.huffingtonpost.com/hamza-tahiri/how-do-you-recyle-a-solar-panel-b_4648903.html The Guardian, "Are solar panels the next e-waste?", 3 September 2010, accessible at http://www.theguardian.com/environment/2010/sep/03/solar-panels-ewaste

12. European Commission DG Research and Innovation, Why socio-economic inequalities increase? Facts and policy responses in Europe, 2010.

13. European Commission DG Research and Innovation, Why socio-economic inequalities increase? Facts and policy responses in Europe, 2010: wage gaps between workers with permanent and temporary contracts can be very significant reaching over 37% in Sweden or 28% in France.

14. United States National Intelligence Council, Global Trend 2030, 2012.

15. Christine Lagarde, 'Towards the next era of growth – reforms and rebalancing' address by the Managing Director of the IMF, International Economic Forum of the Americas, 9 June 2014.

16. European Commission, Europe 2020, 2014: In line with the recommendations from the EU growth and employment strategy, available at http://ec.europa.eu/europe2020/index_en.htm

17. International Monetary Fund (IMF), World Economic Outlook 2014, April 2014.

18. United States National Intelligence Council, Global Trend 2030, 2012.

19. World Bank, China 2030, 2013: China is the world's second largest economy since 2010. China overtook the United States as the world's largest saver in 2008 (according to United States National Intelligence Council, Global Trend 2030).

20. United States National Intelligence Council, Global Trend 2030, 2012: China overtook the United States as the world's largest saver in 2008.

21. United States National Intelligence Council, Global Trend 2030, 2012.

22. Indonesia in 1998

23. Bolivia in 2000

24. Chatham House, The Shale Gas Revolution: Developments and Changes, August 2012: "horizontal drilling and hydraulic fracturing (fracking), where water, sand and chemicals are injected into the horizontal borehole of the well at very high pressure to fracture the shale rocks and release the gas"

25. The Guardian, "Why food riots are likely to become the new normal", 6 March 2013, accessible at http://www.theguardian.com/environment/blog/2013/mar/06/food-riots-new-normal

26. A virtual currency has been defined by the European Central Bank as a type of unregulated digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community.

27. Additional information on virtual currencies can be found in the Europol i-OCTA 2014, accessible at http://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta/

28. Cryptocurrencies are virtual currencies that use cryptography for security and to prevent counterfeiting

29. Bloom & Boersch-Supan & McGee & Seike, "PGDA Working Paper No. 71", 2011, accessible at http://www.hsph.harvard.edu/pgda/working.html

30. Cuaresmy & Labajz & Pružinskýx, Prospective Ageing and Economic Growth in Europe, 2014, accessible at http://eprints.wu-wien.ac.at/4080/1/wp165.pdf

31. Miceski & Stojovska, "Comparative Analysis of Birth Rate and Life Expectancy in Macedonia, Turkey and the European Union", Working Papers, International Conference on Eurasian Economies 2014

32. Van Dijk, The world of crime, Sage Publications Inc., 2008

33. See the forward looking example of FIU.NET ma[3]tch technology, https://www.fiu.net/fiunet-unlimited/match/match3

34. Eurosur is an information-exchange system designed to improve management of the EU external borders, http://frontex.europa.eu/intelligence/eurosur

35. The European Monitoring Centre for Drugs and Drug Addiction, http://www.emcdda.europa.eu/

36. Maritime Analysis and Operations Centre – Narcotics, http://www.maoc.eu/

37. https://www.europol.europa.eu/content/operation-archimedes

38. SIENA (SECURE INFORMATION EXCHANGE NETWORK APPLICATION) is a state-of-the-art tool designed to enable swift, secure and user-friendly communication and exchange of operational and strategic crime-related information and intelligence between Europol, Member States and third parties that have cooperation agreements with Europol.

39. 27 June 2014, document No EUCO 79/14;

40. (1) facilitating the fight against illegal immigration; (2) the fight against trafficking in human beings within the EU and trafficking in human beings from the common countries of external origin for labour exploitation and sexual exploitation purposes; (3) combating the counterfeiting of goods; (4) the fight against excise tax and VAT fraud; (5) combating the manufacture of synthetic drugs and the fight against their smuggling in the EU; (6) the fight against illegal import and distribution of cocaine and heroin within the EU; (7) the fight against cybercrime; (8) combating weapon trafficking; (9) combating organised crime in the area of property

41. The EU Strategy towards the Eradication of Trafficking in Human Beings 2012-2016, 19 June 2012, COM(2012)286;

42. See the Eurojust outcome report A multidisciplinary approach to organised crime: administrative measures, judicial follow-up and the role of Eurojust, Copenhagen, 11-13 March 2012 (Council document 11298/12, Brussels 14 June 2012).

43. See the Report from the Eurojust Strategic Seminar on Cross-border excise fraud: "Emerging threats in the European Union", The Hague, 14-15 November 2013 (doc 8616/14).

44. Proposal for a Council Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering and terrorist financing (COM(2013) 45 final. Strasbourg, 5.2.2013).

45. Council Decision 2002/494/JHA setting up a European network of contact points in respect of persons responsible for genocide, cases against humanity and war crimes (OJ L 167, 26.6.2002, p. 1) and Council Decision 2003/335/JHA of 8 May 2003 on the investigation and prosecution of genocide, crimes against humanity and war crimes (OJ L 118, 14.5.2003, p12).

46. Directives on the right to information in criminal proceedings, OJ L 142, 1.6.2012, p1; the right of access to a lawyer, OJ L 294, 6.11.2013, p1; the right to interpretation and translation, OJ L 280, 26.10.2010, p1.

47. See the Eurojust reports Strategic Project on: Enhancing the work of Eurojust in drug trafficking cases (Jan 2012) and Strategic Project on: Eurojust's action against trafficking in human beings (Oct 2012). Both available on the Eurojust website.

EUROPOL

Eisenhowerlaan 73
2517 KK The Hague
The Netherlands

PO Box 90850
2509 LW The Hague
The Netherlands

www.europol.europa.eu

 www.facebook.com/Europol
 @Europol_EU
 www.youtube.com/EUROPOLtube