The Future of Organised Crime

Challenges and Recommended Actions

1. Current Situation

Law enforcement in the EU has made **progress in intelligence coordination and joint investigation** of crimes that are already considered to be priorities. But we have a more limited capacity for monitoring crimes which do not meet this threshold, and for anticipating new trends.

The conservative and **reactive nature of policing** and ever tightening budgets leave agencies insufficiently prepared for new threats. Having enjoyed a monopoly on crime fighting for many years, we remain good at policing what we are comfortable with, but our resistance to change means that we risk developing blind spots for those crimes that we do not routinely investigate.

Cybercrime is a prime example of this. While technology changes on a daily basis, law enforcement often relies on doing what it has always done. Criminals keep one eye on the horizon, but legislation struggles to keep pace and lack of harmonisation sometimes prevents concerted efforts and timely responses from Member States. For all types of criminal activity, asymmetry in legislation and regulatory policy results in displacement, not only between Member States, but between the EU and other parts of the world.

Moreover, the very criminal activities which are identified as being some of the most pressing, lucrative and **rapidly evolving** – such as fraud and cybercrime – are those which until now have received comparatively little concerted law enforcement attention or resources. Where marked progress has been made in stepping up the investigation of cybercrime, this has often been achieved at practitioner level. Given the **financial constraints** under which we all currently operate, we need to consider smarter ways of working.

2. Challenges and Future Risks

Changes in the wider global environment will provide new opportunities for criminal activity. **Demographic shifts** such as an ageing EU population are likely to prove fertile ground for labour migration, raising the possibility of increased trafficking in human beings (THB) for labour exploitation and the facilitation of illegal immigration. In addition, **geopolitical unrest** outside the EU has the potential to create large diaspora communities that are isolated, excluded from mainstream employment, and therefore vulnerable to the influence of criminal groups.

Economic disparity also will continue to bring individuals into greater proximity to organised crime. Poverty, in some cases aggravated by the global economic crisis, has the potential to swell the workforces of criminal groups with not only migrants, but also EU citizens. Projected food crises and other disruptions to supply chains will also fuel markets for counterfeit and stolen goods.

Meanwhile, criminal groups will continue to spot opportunities in **emerging markets** such as alternative energy supply and infrastructure, trade in rare minerals and the disposal of toxic waste, with the risk of monopolisation in markets in which there are large incentives, and which are not subject to sufficient scrutiny or competition from legitimate investors. Equally, illicit activity will continue to have a negative effect on legitimate markets. One example of this is the alleged contribution of metal theft to fluctuating metal prices.

Lack of synergy between law enforcement and **legislative bodies** enables criminals to exploit loopholes and capitalise on demand for illicit commodities. In some cases, controls and regulatory frameworks have themselves proved to be criminogenic. Moreover, the length of time it can take to bring suspects to trial can preclude a timely judicial response, thereby reducing its effectiveness as a deterrent.

The further development of the **Internet and related technologies** will not only put new tools at the disposal of all criminal groups, but will also expose new vulnerabilities in our information society. A future convergence of “entry level” criminal tools and a new generation of technically capable youth raises the possibility of online petty crime. In addition, there is likely to be an increasing overlap between organised crime and terrorist activity on the Internet. Both recent hacktivist attacks on corporations and government websites, and the appearance of tools specifically designed to interfere with the control systems of critical infrastructure (Stuxnet), indicate that this will be a key concern for the future.

The **mass of data** available for investigation, especially pertaining to cybercrime and economic crime, is a clear challenge to established law enforcement capability. It is already no longer possible or efficient to seek to identify and prosecute all suspects for these crimes. At the same time, the volume of this information is expected to expand considerably, as is its role as a commodity from which criminal groups can profit, particularly in light of increased data storage in “the cloud” and a persistently upward trend for use of social media. A more innovative approach is required, with greater emphasis on disruption, prevention and problem solving.

3. Recommended Actions

We must gear up in the fight against organised crime, not only in order to optimise our responses today, but also to prepare ourselves for the challenges of the future. A joined up world requires a crime fighting approach which is equally joined up. A new model of policing is suggested that draws on a network of law enforcement specialists, and emphasises **collaboration with partners in the private sector, NGOs and academia**.

Under this new model, joint threat and risk assessments bringing together a **range of EU security actors** such as Europol, Frontex, SitCen, and ENISA, should provide comprehensive 360 degree analysis of criminal phenomena. In terms of turning strategic findings into operational activity, Project Harmony will do this for crime phenomena that are already subject to law enforcement prioritisation.

We also now need to have a more coordinated approach to traditionally less visible, but no less damaging, phenomena such as fraud and cybercrime. This is not merely a question of financial resources, but of sourcing the **expertise**, and providing the **tools and training** necessary to successfully combat these activities and anticipate their evolution.

Changes in the criminal landscape require changes in law enforcement skill sets. In order to drive forward the fight against organised crime, officers, including Chiefs of Police, must have **greater awareness** of emerging and less visible types of criminal activity, such as cybercrime and economic crime. Investigation tools should be standardised wherever possible, and knowledge of how to exploit virtual resources such as social media should be a **minimum requirement** for the investigation and disruption of organised crime. The judiciary should also be a priority for awareness raising on non-traditional crimes.

More generally, there needs to be clear acknowledgement of the interconnections between global risks and the threat posed by criminal groups, and not merely in the context of assessment. This interconnection demands an **integrated approach to strategic planning** at EU level, with both greater levels of foresight and greater synergies between security planning and economic, energy, social and other frameworks. In particular, those involved in the development of legislative and regulatory frameworks should consult law enforcement with the aim of **crimeproofing** future legislation. There is also consensus amongst experts in a number of different investigative fields that the EU requires **analysis** which goes beyond law enforcement's traditional scope and the envisaged cycle of the SOCTA, to provide Member States and partners with longer range strategic foresight on global issues related to criminal activity.

Public-private partnership is key to our collaborative response, not least because of its global ethos and reach. A first step would be to disseminate the EU's strategic analysis to the private sector to raise awareness, but the primary objective is to minimise vulnerabilities in legitimate markets. Key players in online service provision and the financial sector should be prioritised for outreach for the purposes of information sharing and minimising vulnerabilities in emerging technologies.

In summary, the working group on organised crime advocates a **more creative approach** to combatting criminality that looks beyond traditional law enforcement investigations, prosecutions and surveillance methods, and encompasses a wide range of **administrative and preventative measures**, including serious crime prevention orders already in use in some Member States.

Recognising that the generation of profit is an important motivation for criminal groups, **asset recovery** and financial investigation capabilities must be strengthened, to increase the risk to criminal proceeds. Specific measures such as the establishment of a common EU platform for confiscation, financial reporting orders, and reversal of the burden of proof should also be considered as tools for reducing the rewards of organised crime.

In light of the increasingly blurred distinction between internal and external security, EU law enforcement would benefit from expanding its support and promotion of intelligence-led investigation in developing countries and other areas of the world whose criminal groups impact on Member States. More generally, good practice should be shared on initiatives for **capacity building** in fragile states, with a view to preventing significant infiltration by criminal groups.

Last, but by no means least, we have an unprecedented opportunity to work in partnership with the **citizens of the EU**. The use of Internet services such as social media to generate community intelligence and distribute crime prevention guidance would not only provide reassurance, but would also empower the public to assist law enforcement in the fight against organised crime.