

# Organised crime in Europe: Emerging trends and policy challenges

## Summary

Serious and organised crime inflict huge costs on both the EU economy and society. Organised crime is an increasingly dynamic and complex phenomenon, as it has become more interconnected, transnational and digital. The Covid-19 pandemic has led to an increase in cybercrime, fraud and counterfeiting. Police and judicial actions and the effective implementation of existing EU instruments are critical in tackling this challenge. New strategies to disrupt the business models and structures of criminal organisations will also benefit from an integrated approach, recognising the socio-economic, technological and geopolitical dimensions of the problem.

## Background

Organised crime damages lives and communities, and the [cost to the EU economy](#) is considerable. [In 2019](#), criminal revenues in the main criminal markets amounted to €139 billion, or 1 % of the EU's GDP. Organised crime groups (OCGs) increasingly engage in several categories of criminal activity, rather than just one. As of 2021, 80 % of OCG activities involved drug trafficking, organised property crime, various types of fraud, and crimes exploiting people as a commodity. OCGs have become more violent: over 60 % use violence as part of their *modus operandi*. The rapidly evolving nature of crime brings new threats, and this prompts renewed debate on how the EU – in cooperation with Member States and relevant EU agencies – should respond.

## Main trends

### The rise of cybercrime

Cyber-dependent crime has increased dramatically, as criminal networks take advantage of vulnerabilities accompanying globalisation, digitalisation, and the development of new technologies. Cyber-criminals were quick to [adapt their methods](#) to changes brought by the pandemic. Groups used malware and ransomware to capitalise on the increase in remote working and in online transactions, while also refining their target selection and strategies. Many criminal activities shifted to the online domain; 2021 saw a rise in the use of technologies by criminals, for communication, transactions and other purposes. The rise of [cryptocurrencies](#) also creates new law enforcement challenges, as they can enable criminal activity. They are fast, accessible, borderless, and offer anonymity to transaction makers. As with other technological innovations, the time it takes to update the regulatory environment leaves room for predatory operators. The development of effective regulatory, organisational and technical resources and responses, at national, EU and international levels, is necessary to halt the spread of cyber-dependent crime.

### Expanding corruption networks

Corruption remains a key element of organised crime. Most criminal groups use corruption networks to develop and protect their illegal activities. Europol reports that 60 % of criminal networks in the EU engage in various forms of corruption, and that more than 80 % use legal business structures to carry out or to hide criminal activities. Corruption is found in both the public and the private sectors, but it often goes undetected. A majority of EU citizens believe corruption is either [worsening or stagnating](#) in their countries, according to Transparency International (TI). TI has also reported significant differences in the effectiveness of anti-corruption strategies across the EU, with important gaps in some EU Member States. Corruption erodes the rule of law, weakens institutions and hinders economic development. Stronger coordination and action at EU level can supplement national law enforcement and criminal justice capabilities, making full use of EU primary and secondary law provisions and instruments (under Title V TFEU).

## An increasingly transnational problem

Transnational criminal networks are increasingly far-reaching and able to adapt to different national contexts. Europol's Serious and Organised Crime [Threat Assessment](#) suggests that almost 70 % of such networks are active in more than three countries: 65 % are composed of members of multiple nationalities. Non-EU criminal groups also operate within the Union's borders; over half of organised criminals active in the EU are thought to be non-EU nationals. All this poses a serious threat to the safety, security, and development of the EU and its citizens. The transnational reach of organised crime in Europe is grounds for [enhancing EU tools and mechanisms](#) to supplement and support the actions of Member States. EU action against organised crime can play a more significant role in future, since it can facilitate cooperation between national and European agencies on matters such as investigations across borders, interoperability, and timely and accurate information sharing.

## Key uncertainties

The European Commission last year presented the [EU strategy](#) to tackle organised crime in 2021-2025, to enhance the EU's ability to support Member States in this area. The strategy sets out the tools and measures needed to disrupt the business models and structures of criminal organisations across borders, both online and offline. Success will depend on the speed at which the strategy's key measures are launched, and the effectiveness of their implementation. Organised crime has proved to be dynamic and adaptable, and it seeks to exploit vulnerabilities and gaps in law enforcement across the EU. A pivot towards proactive methods embedded in long-term strategies can also improve the authorities' ability to respond to both current and future threats.

The EU strategy builds on the premise that the evolution of criminal networks can be traced to socio-economic and technological developments, among other factors. It follows that action against criminal networks is unlikely to succeed in a vacuum, or on the basis of law enforcement alone. Policies to reduce both socio-economic stress and technological vulnerabilities have a role.

When geopolitical tensions are added to economic distress, conditions become even more favourable for organised crime. Criminal activities tend to become more prominent in [conflict areas](#) and in disputed territories. The [absence](#) of law enforcement and legal capacity leaves room for criminals to develop and conduct operations. Geopolitical instability has already brought higher crime rates in conflict zones in the EU neighbourhood, such as [Crimea](#), [Donbas](#), [Transnistria](#) and the [Western Balkans](#). Such trends point to a need for greater attention to the dangers of economic and geopolitical developments facilitating organised crime – and vice versa.

## Possible disruptions

A worst-case scenario would be the spread of OCG influence on government and administration. Parts of the continent are [already affected](#) by this; in some localities, criminal elites occupy leadership roles in public administration. If this leads to the integration of criminal elements into judicial and law enforcement systems, it creates a serious threat to stability and development both in the affected areas and in neighbouring regions. This would increase the damage done by underground networks, and undermine the cohesion and integrity of the EU.

## Conclusion

Criminal groups adapted very quickly to the circumstances of the pandemic, and will seek to take advantage of economic downturns, depressed income levels and rising geopolitical tensions. Yet the EU has the potential to better prepare for future threats. It can draw on Treaty provisions, a range of law enforcement and judicial instruments, [multidisciplinary initiatives](#) and proactive strategies to reduce vulnerabilities and gaps in different parts of the Union. Anticipatory governance and strategic planning can also help, by underlining the benefits of combining law enforcement with efforts to tackle socio-economic root causes of recruitment into crime, and with improvements in cybersecurity in both the public and private sectors.

