Council of the European Union

Brussels, 23 June 2026
(OR. en)

9989/26

COPEN 215
EJN 6
JAI 711

NOTE

From:	General Secretariat of the Council
To:	Delegations
Subject:	Conclusions of the 65th plenary meeting of the European Judicial Network (EJN) (Copenhagen, 5-7 November 2025)

Delegations will find attached the above-mentioned conclusions, relating to the topics of combatting criminal organisations, crime as a service and crypto assets.

65th PLENARY MEETING OF THE EUROPEAN JUDICIAL NETWORK

5-7 NOVEMBER 2025

COPENHAGEN, DENMARK

Conclusions on

Combatting Criminal Organisations

(Workshop 1)

The 65th Plenary Meeting of the European Judicial Network (EJN) in criminal matters was hosted in Copenhagen by the Danish Presidency of the Council of the EU in collaboration with the EJN Secretariat on 5-7 November 2025.

Background

As organised and transnational crime committed by gangs and criminal networks remains a significant challenge with serious human and societal impacts, one of the priorities of the Danish Presidency was the fight against serious cross-border and organised crime.

In line with this priority of the Danish Presidency, one of the workshops on the agenda of the EJN Plenary Meeting concerned combatting criminal organisations.

Combatting criminal organisations is also a priority for the EU. Thus, the European Commission's Drugs Strategy 2021–2025 states that one of the strategic priorities is to "disrupt and dismantle high-risk drug-related organised crime groups operating in, originating in or targeting the EU Member States". On 8 July 2025, the Commission presented an evaluation of the strategy and action plan. It states that "Concrete proactive measures are needed to tackle the organised drug crime, disrupt their [drug-related organised crime groups] activities and tackle their infiltration into EU's supply chain using violence and corruption." Furthermore, the Commission's internal security strategy of 1 April 2025, "ProtectEU", states that the Commission will work in close cooperation with the Member States to propose a new EU Drugs Strategy and that the Commission will present a legislative proposal for modernised rules on organised crime in 2026.

Overview

The Member States have each taken different measures in the fight against criminal organisations, and national legislation in each Member State offers different options for combatting criminal gangs and other criminal organisations. In the workshop, participants shared experiences, challenges and best practises in combatting criminal organisations.

Legal definition of "a criminal organisation"

In the workshop, the vast majority of Member States reported having a definition of *"a criminal organisation"*. However, the criteria applied varies from Member State to Member State.

Only a few Member States reported not having a definition of "a criminal organisation". In one of these Member States, there was an ongoing discussion on introducing a definition. Another Member State reported that, while not having a definition of "a criminal organisation" in national legislation, the definition was derived from the Member State's extensive case law in the field.

A summary of the various contributions showed, that the Member States shared the understanding of "a criminal organisation" as an organisation that needs to be structured over a certain period of time and to be engaged in committing criminal offences.

It emerged from the discussions in the workshop that *"participating in a criminal organisation"* is a separate crime in certain Member States, while in others it is an aggravating circumstance that is reflected in the penalties applied. In some other Member States it is a separate crime *and* an aggravating circumstance as well.

Legal provisions on "dissolution and prohibition" of a criminal organisation

Participants reported that several countries have provisions on dissolution and prohibition of a criminal organisation, such as closing the criminal organisation down or preventing the members of the criminal organisation from meeting. However, certain Member States can take those measures only in relation to a legal entity.

It was highlighted that the territorial limitation of the dissolution or prohibition measures taken by a Member State in relation to a criminal organisation has no cross-border effect other than the possibility that the criminal organisation may relocate to another Member State in order to pursue its criminal activities. This was highlighted as a particular limitation on the effectiveness of such measures.

Procedural aspects

In almost all participating Member States, responsibility for the burden of proof lies with the public prosecutor, who presents to the court evidence of the criminal organisation or of the perpetration of crime. In common law countries – Ireland, Cyprus and Malta – the responsibility for the burden of proof lies with the police.

What differs in the Member States is whether the evidence is presented to the judge in an oral hearing, by written submissions, or a combination of both.

When tackling cross-borders organisations, a particular consideration is the employment of undercover agents, the requirements for their use and functioning, and how their identity is handled. Some participants noted that there is lack of common requirements for the use of cross-border undercover agents, and therefore, further discussions in this field may be relevant.

Another pertinent point in this regard to consider when tackling criminal organisations was, according to the participants, how to deal with threats to witnesses and the legal remedies available.

International cooperation – tackling the same criminal organisation

In the workshop, it was considered a possibility that Member States may simultaneously be tackling the same criminal organisation operating cross-border, and without the Member States being aware of the investigation of another Member State. It was recognised that there is a need for Member States at all levels to cooperate and exchange information, for example information on criminal offences committed by criminal organisations, information on investigations and prosecutions against criminal organisations, and information on the prohibition of criminal organisations.

Participants concluded that by exchanging information each Member State could build on the information, knowledge and expertise that they have already acquired. It was suggested that the creation of a new tool such as a *"black list"* of criminal organisations banned in the European Union could be introduced. According to participants this would benefit all Member States. In particular it would enable a Member State, confronted with a criminal organisation for the first time, to gather knowledge about the existence of the criminal organisation and to draw lessons learned from the actions and experiences of other Member States.

Further, participants noted that Member States' timely sharing information about the modus operandi of a criminal organisation, which may be characterised by flexibility and changing tactics, provides other Member States with knowledge on how the criminal organisation evolves on the ground. Such information may be key in combatting the criminal organisation.

The role of the European Judicial Network (EJN)

The workshop recognised the role of the EJN as being crucial to the sharing of judicial decisions in the field of combatting criminal organisations.

Further, the workshop supported the idea of identifying EJN Contact Points with specific expertise in combatting criminal organisations and indicating such expertise in the EJN Contact Point list.

Conclusion

In the workshop, participants shared information on, among other things, Member States' definition of "a criminal organisation" and legal provisions on dissolution and prohibition of criminal organisations. Participants emphasized the importance of Member States' sharing of information on for example criminal offences committed by criminal organisations, investigations and prosecutions against criminal organisations, and the prohibition of criminal organisations. Further, it was suggested to introduce a new tool such as a *"black list"* of criminal organisations banned in the European Union. Finally, the workshop recognised the role of the EJN as being crucial to the sharing of judicial decisions in the field of combatting criminal organisations, and supported the idea of identifying EJN Contact Points with specific expertise in combatting criminal organisations and indicating such expertise in the EJN Contact Point list.

65th PLENARY MEETING OF THE EUROPEAN JUDICIAL NETWORK

5-7 NOVEMBER 2025

COPENHAGEN, DENMARK

Conclusions on

Crime as a Service

(Workshop 2)

The 65th Plenary Meeting of the European Judicial Network (EJN) in criminal matters was hosted in Copenhagen by the Danish Presidency of the Council of the EU in collaboration with the EJN Secretariat on 5-7 November 2025.

Background

As organised and transnational crime committed by gangs and criminal networks remains a significant challenge with serious human and societal impacts, one of the priorities of the Danish Presidency was the fight against serious cross-border and organised crime.

In this regard, it was a priority for the Danish Presidency to support the work of relevant EU agencies and to strengthen cooperation within the EU and with third countries in the fight against organised crime.

Persons behind serious cross-border crime often take residence in third countries. Therefore, the Danish Presidency focused also on judicial cooperation with third countries, in particular regarding the extradition of persons suspected or convicted of committing organised crime.

In line with these priorities, the topic in one of the workshops of the EJN Plenary Meeting was Crime as a Service.

Overview

In the workshop, participants discussed the legal and practical challenges in investigating and prosecuting Crime as a Service cases, where criminal organisations are frequently putting criminal assignments up for tender. The assignments are usually advertised in groups on the darkweb but sometimes also on social media groups through advertisements in which criminals advertise for someone willing to take on a given criminal assignment for a fee. Interested parties can apply for the 'job' by answering the advertisement.

Participants agreed that they encounter more and more investigations involving such modus operandi, where advertisements are published online for different types of crimes, for example homicide and severe bodily harm, but also cybercrime and drug trafficking. They noted that very often such crimes have a cross-border element where the exchange of information and documents between law enforcement and judicial authorities is essential for a successful investigation and prosecution.

The terms "Crime as a Service" and "Violence as a Service"

The workshop focused, among other things, on the terms "Crime as a Service" and "Violence as a Service". Participants noted that the term "Crime as a Service" covers a wide spectrum of criminal activity, and often it relates to specialized cybercrime services such as providing malware or ransomware, money laundering services, and drug trafficking, while the term "Violence as a Service" is notably used in relation to physical violence as well as contract killings and bombings.

Criminal liability — Attempt and aiding and abetting

Another core topic discussed in the workshop was the criminal liability for the persons taking part in the criminal activity. These cases typically involve multiple distinct roles: the **instigator** who initially orders and finances the assignment, the **recruiter** who puts the assignment up for tender on behalf of the instigator, the **enabler** who aids and equips the executor (e.g. providing a weapon or tools), and the **executor** who commits the actual offense. Participants discussed two key legal issues stemming from the structure of the criminal activity in Crime as a Service cases:

- **Attempt:** The legal definition of "attempt" varies across the Member States. Intent is always required, but some Member States consider preparatory acts for committing the crime (e.g. scouting a location or procuring materials) sufficient for criminal liability, while others require acts much closer to actual execution. This creates complications especially around the double criminality requirement in surrender and extradition cases.

- **Aiding and abetting:** The core difficulty is proving that the enabler had the specific knowledge or the intent that the executor would commit a particular offense. Participants suggested that preparatory offenses or the offense of participation in a criminal organisation – available in the Criminal Codes of most of the Member States – could help to close the gaps in criminal liability where standard aiding and abetting provisions fall short.

Participants emphasized that due to the differences in the legal definitions in the national laws of the Member States, it is essential that there is a possibility for consultations already at the stage, where the Member States are drafting possible requests for assistance, in order to minimize difficulties at the stage of execution of the requests. The EJN is a fitting channel for such consultations.

Jurisdiction

Crime as a Service cases are frequently transnational, with multiple states potentially having jurisdiction. The discussions showed that most Member States have broad jurisdiction over crimes committed in their territory or affecting their country or citizens. The predominant view established during the discussions was that proceedings should primarily be conducted in the state where the actual offense was committed and the executor acted, as this was generally considered the most efficient approach and best serve the interests and rights of victims. However, participants noted that investigative tactics and practical experience should also be taken into account when deciding where the proceedings should be conducted. Joint Investigation Teams (JITs) were highlighted as particularly valuable in navigating these multi-jurisdictional situations, particularly due to the close cooperation between the judicial and police authorities and the possibility for swift exchange of evidence.

Data retention and encrypted communications

In the workshop, it was agreed that the executor's mobile phone (communication device) was crucial to investigations due to the detailed information, which it usually contains. This issue was flagged as a general concern in many criminal cases, but data retention and access to encrypted communications is pivotal in Crime as a Service cases given that digital communication is absolutely central to how these networks operate and communicate. Law enforcement agencies therefore need three things: data retention by service providers, surveillance of encrypted communications, and easier access to data on seized mobile phones and other devices.

Participants underlined that the challenges in this regard are significant. Data retention rules differ greatly between Member States – some require no storage at all, while others mandate retention for periods ranging from two months to much longer. On seized devices, burner functions and automatic message deletion after a set period are a serious obstacle for investigators. Participants stressed the importance of law enforcement keeping pace with technological innovation, acknowledging that this is not always easy.

International judicial cooperation and the role of the EJN in supporting national authorities

Participants emphasized that investigating and prosecuting Crime as a Service cases nearly always require international judicial cooperation. They also highlighted that intelligence sharing is key. Direct and informal contacts – especially through the EJN Contact Points – were emphasized as essential for speeding up mutual legal assistance, surrenders and extraditions linked to criminal investigations. Thus, the role of the EJN Contact Points as "active intermediaries" in judicial cooperation remains central for bridging the national authorities conducting the investigations and prosecutions.

Further, due to the cross-border nature of the criminal phenomena where perpetrators are hired from around the world, the participants underlined that direct contact with contact points from other regional judicial networks is essential for timely transmission and execution of mutual legal assistance, surrender and extradition requests as well as for detecting parallel investigations.

Conclusion

The workshop discussed the legal and practical challenges in investigating and prosecuting Crime as a Service cases and agreed that they encounter more and more investigations involving such modus operandi. Participants noted that very often such crimes have a cross-border element where the exchange of information and documents between law enforcement and judicial authorities is essential for a successful investigation and prosecution. Further, data retention by service providers, access to encrypted communication and data on seized electronic devices are crucial to the investigation and prosecution of Crime as a Service cases.

Participants emphasized that investigating and prosecuting Crime as a Service cases nearly always require international judicial cooperation and the role of the EJN Contact Points as “active intermediaries” in judicial cooperation remains central in such cases.

65th PLENARY MEETING OF THE EUROPEAN JUDICIAL NETWORK

5-7 NOVEMBER 2025

COPENHAGEN, DENMARK

Conclusions on Crypto Assets (Workshop 3)

The 65th Plenary Meeting of the European Judicial Network (EJN) in criminal matters was hosted in Copenhagen by the Danish Presidency of the Council of the EU in collaboration with the EJN Secretariat on 5-7 November 2025.

Background

One of the priorities of the Danish Presidency was the fight against serious cross-border and organised crime. Another priority was the misuse of new technologies for criminal or harmful purposes. In line with these priorities, the Danish Presidency chose in close collaboration with the EJN Secretariat to focus one of the workshops of the EJN Plenary Meeting on crypto assets.

Crypto assets are used to an increasing extend by criminal players, including criminal organisations and cyber criminals. As is the case with traditional funds generated by criminal activity, crypto assets are often channelled to third countries. This circumstance combined with the fact that crypto assets can be moved very quickly makes it difficult to seize and confiscate crypto assets.

Overview

The workshop focused on the increasing role of crypto assets in criminal activity and the challenges they present for investigators and prosecutors as well as other judicial authorities.

Participants noted that while crypto assets were initially associated primarily with organised crime, **they are now encountered across a broad range of offences and are becoming an increasingly common tool used by criminals.**

The workshop highlighted that virtually **all types of crime may involve crypto assets**. Examples discussed included money laundering, cybercrime, ransomware attacks, online fraud, investment fraud, human and drug trafficking, child sexual exploitation offences, and the emerging phenomenon of "Crime as a Service".

Crypto assets **may be used both as a means of payment and as a mechanism for concealing or transferring criminal proceeds**. Participants observed that the number of investigations involving crypto assets continues to increase steadily and that **such cases almost always contain a cross-border dimension.**

Key challenges

A significant part of the discussion focused on the challenges faced by practitioners.

1. The borderless nature of crypto assets frequently **requires complex cross-border investigations** involving multiple jurisdictions and different legal systems.

2. Participants noted that Member States often **apply different approaches to obtaining information, freezing assets and carrying out confiscation measures**.

3. Participants also noted that Member States have different views regarding **cooperation with crypto-asset service providers (CASPs),** including whether and under what conditions authorities may directly contact service providers located in another jurisdiction.

4. The workshop further highlighted **difficulties arising from opaque corporate structures, non-cooperative service providers and situations where the actual location or legal establishment of a CASP** is difficult to determine.

5. Some participants also noted the lack of a common operational approach across Member States and discussed the **potential relevance of existing and future EU instruments, including the e-Evidence framework.**

6. Another recurring theme was the **need for specialised expertise**. Crypto-asset investigations require a combination of legal, financial and technical knowledge that is not yet sufficiently widespread among investigators, prosecutors and judges. Limited familiarity with blockchain technology, available investigative tools and asset-tracing techniques remains a practical obstacle in many jurisdictions.

Best practices identified

Despite these challenges, participants identified a number of practical approaches that can contribute to more effective investigations.

1. A key message emerging from the discussions was the **importance of early action.** Given the speed with which crypto assets can be transferred across borders and platforms, the immediate preservation and securing of assets was considered essential.

2. Participants also emphasised the value of involving **specialised experts from the earliest stages** of an investigation, including during searches and when executing European Investigation Orders (EIOs) or Mutual Legal Assistance (MLA) requests (for example digital forensic experts present “on the spot” during house searches).

3. The use of **standardised forms and preservation templates when communicating with CASPs** was identified as another useful practice capable of facilitating and accelerating cooperation.

4. Participants also referred to the opportunities offered by **Directive (EU) 2024/1260, the new EU Asset Recovery and Confiscation Directive**, including the possibility of pre-confiscation sales in appropriate cases.

5. **Effective cross-border cooperation** was considered one of the most important factors in successfully investigating and recovering crypto assets. In this regard, the workshop underlined the importance of making full use of **existing cooperation mechanisms and specialised networks**. Particularly, reference was made to the support available through the EJN, Eurojust, Europol, Joint Investigation Teams (JITs), Camden Assets Recovery Inter-agency Network (CARIN), SIRIUS project (Cross-border Access to Electronic Evidence) and the European Judicial Cybercrime Network (EJCN). In addition, these networks are also essential for identifying competent authorities quickly.

Role of the EJN

Participants discussed how the EJN could further support practitioners dealing with crypto-asset cases.

1. Several proposals were put forward, including the **preparation of dedicated Fiches Belges on crypto assets** containing practical information on national legal frameworks and practices, extending beyond freezing and confiscation issues alone.

2. The workshop also supported the idea of **identifying EJN Contact Points with specific expertise** in crypto assets and indicating such expertise in the EJN Contact Point list.

3. In addition, participants highlighted the need for **targeted training activities on crypto assets and blockchain technology**, as well as practical handbooks and guidance materials tailored specifically to prosecutors and judges.

Conclusion

The workshop concluded that crypto assets are becoming an increasingly important feature of criminal investigations and asset recovery proceedings. While significant legal, technical and operational challenges remain, participants agreed that enhanced expertise, early intervention, effective cross-border cooperation and better use of existing networks and tools will be essential to addressing the growing role of crypto assets in criminal activity. The discussions also highlighted a clear need for continued training, practical guidance and stronger cooperation mechanisms to support practitioners dealing with this rapidly evolving field.