Council of the European Union

Brussels, 14 February 2025
(OR. en)

5835/25

LIMITE

COSI 16
ENFOPOL 36
CRIMORG 20
IXIM 20
MIGR 46
ASIM 14
FRONT 33
COPEN 15
CATS 3
SCHENGEN 7
RELEX 121
JAI 128
COMIX 36

NOTE

From:	Presidency
To:	Delegations
Subject:	Preventing and combatting migrant smuggling in the digital age – *Exchange of views*

DOCUMENT PARTIALLY ACCESSIBLE TO THE PUBLIC (08.04.2025)

Introduction

Geopolitical and socioeconomic instability worldwide, as well as climate change, are expected to keep driving migratory movements. Migrant smuggling is a key activity for criminal networks operating inside and outside the EU, sustained by continued demand for facilitation services. Many of those who willingly pay smugglers to help them cross borders do so at great personal risk. In 2023 alone, 382 000 illegal border-crossings on entry were reported at the EU's external borders to by Frontex[1]. Even if a substantial drop in irregular border crossings can be seen in 2024, migrant smuggling is still a high-profit, low-risk business for criminal networks.

1 WK 13476/2024: Frontex Cross-Border Crime Threat Assessment, 2024.

Around 6% of the most threatening criminal networks identified at EU level were exclusively involved in migrant smuggling[2]. The criminal networks involved in migrant smuggling are increasingly sophisticated, professional and violent. Migrant smugglers offering 'safe trips' online are ruthless in their lack of respect for the safety and lives of irregular migrants. This has resulted in many tragic incidents during both sea and land crossings: according to the International Organization for Migration (IOM), over 72 400 irregular migrants have reportedly lost their lives, with over 8 200 in 2024 alone, marking the second highest number since 2016[3].

Migrant smuggling facilitated by digital means: a rising threat

Migrant smugglers have quickly adjusted their modus operandi to benefit from the opportunities offered by digital technologies, which have become an integral part of their business model. Digitalisation boosts all aspects of this crime and enables criminal actors to become more efficient, agile and resilient against law enforcement intervention, e.g. by taking advantage of encrypted communication solutions and easily accessible digital tools.

Migrant smugglers use mainstream social media platforms to advertise their services, often misleadingly, presenting smuggling routes as safe. Social media are also used to recruit facilitators and to communicate with potential victims. The perpetrators spread disinformation online about migration policies and routes or the risks involved, to attract vulnerable individuals. The use of widely available artificial intelligence (AI) tools, including the creation and dissemination of deepfakes and automated translation tools, might provide new opportunities for criminals to reach more diverse target groups to lure potential clients and increase demand for smuggling services.

---

2 Europol (2024): the EU's most threatening criminal networks, accessible at https://www.europol.europa.eu/publication-events/main-reports/decoding-eus-most-threatening-criminal-networks, retrieved on 11.2.2025

3 Data | Missing Migrants Project

Criminal networks abuse the protection provided by freely available end-to-end encrypted interpersonal communications services such as instant messaging applications, which they use for the exchange of operational details to coordinate and plan their activities without a significant risk of being detected by law enforcement. In recent years, despite the creation, transmission and storage of ever greater quantities of data by users and providers, effective access by law enforcement to this data has emerged as a key challenge in conducting investigations and prosecutions into criminal offences and effectively enforcing the law on migrant smuggling. Differences in national data retention rules in the EU are relevant in this context[4].

Online campaigns launched by migrant smuggling networks to recruit collaborators have a wide geographic scope and can simultaneously target multiple nationalities in one call. In their advertisements, the smugglers provide detailed information on work conditions and promise lucrative financial rewards and various other advantages, such as support in case of apprehension, the provision of vehicles and accommodation.

While cash payments still prevail as the preferred means of payment in migrant smuggling, the use of Hawala banking systems in conjunction with cryptocurrencies allows smugglers to exploit both traditional and modern methods to transfer and receive payments and to launder their profits, while preserving anonymity. There is a significant gap in awareness and training among law enforcement regarding digital aspects of migrant smuggling, including cryptocurrency techniques and the dark web's role.

[4] The development of a common EU legal framework for data retention for the purpose of criminal investigations and prosecutions of cross-border crimes – including migrant smuggling related offence – is an important step to ensure the efficiency of the criminal justice system in the digital age. This was one of the main findings of the second Data Retention Report jointly prepared by Eurojust and the European Judicial Cybercrime Network (EJCN) in November 2024.

EU tools to mitigate the threat of migrant smuggling in the digital age

Effectively tackling migrant smuggling requires a holistic approach which must encompass, among others: cooperation with countries of origin and transit, with both law enforcement and the judiciary; the use of advanced technologies to disrupt criminal networks; information sharing; and a strong regulatory framework.

The renewed EU action plan against migrant smuggling (2021–2025) adopted a comprehensive approach and sought closer cooperation with partner countries along the migratory routes towards the EU and with international organisations, including through anti-smuggling operational partnerships. It supported the implementation of legal frameworks sanctioning smugglers active within and outside the EU. While building on the EU action plan 2015-2020, it addressed the digital angle through capacity building and training for specialised investigators and judicial authorities provided by Europol, the European Union Agency for Law Enforcement Training (CEPOL) and the European Judicial Training Network, including under the auspices of the European Multidisciplinary Platform Against Criminal Threats (EMPACT).

To bolster the EU response to migrant smuggling, the Commission launched the Global Alliance to Counter Migrant Smuggling in November 2023. In this framework, a thematic conference on tackling migrant smuggling in the digital domain was organised by the Commission together with Europol, supported by Eurojust, in April 2024. The conference discussed the need for strengthened law enforcement cooperation on tackling migrant smuggling online, wider awareness of the added value of using digital evidence in migrant smuggling cases as well as sharing information and good practices, including the SIRIUS project, implemented by Europol and Eurojust in relation to cross-border access to electronic evidence. DELETED

Since its establishment in 2016, Europol's European Migrant Smuggling Centre (EMSC) has gradually engaged in developing a law enforcement response to online migrant smuggling.

DELETED

The fight against criminal networks involved in migrant smuggling is one of the EU's priorities for the fight against serious and organised crime in the EMPACT cycle 2022-2025.

DELETED

While operational cooperation is essential to effectively combat migrant smuggling facilitated by digital tools, partnerships with the private sector, in particular providers of online services, should also be considered a priority. In this spirit, the Global Alliance to Counter Migrant Smuggling also includes a call for online service providers to work together with the relevant public authorities to identify and take down online content that publicly instigates people to migrate irregularly or promotes illicit activities related to the smuggling of migrants.

The EU Internet Forum is a good example for the creation of a collaborative environment for EU Institutions and Member States, the internet industry and other partners to discuss and address the challenges posed by malicious and illegal content online. Launched by the Commission in December 2015 with the initial objective of addressing the misuse of the internet for terrorist purposes with a focus on the dissemination of illegal content[5], its scope of activities has gradually expanded to also cover child sexual abuse, drug trafficking and trafficking in human beings. Given the increasing misuse of online services for migrant smuggling purposes, the EU Internet Forum could explore responses to that abuse and encourage tech platforms to enhance cooperation with law enforcement in that area. In the senior officials meeting of the EU Internet Forum in December 2024, it was decided to extend the scope of the Forum to include the online dimension of migrant smuggling.

In addition to enhancing the dialogue with private parties, it is also important to ensure the full implementation of the Digital Services Act (DSA)[6], which requires very large online platforms and very large online search engines to report and remove illegal content, including content related to migrant smuggling. In the upcoming partial review of the DSA planned for later in 2025, the Commission could look at the effectiveness of the reporting mechanism under Article 18 DSA with regard to illegal content related to migrant smuggling.

Europol also has a key role in cooperation with private sector stakeholders through the European Cybercrime Centre and the Innovation Lab. In addition, the work of the EU Internet Referral Unit (EU IRU) in detecting malicious content on the internet and in social media could be further strengthened regarding migrant smuggling by providing Europol with the necessary additional resources.

---

5 Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online, OJ L 172, 17.5.2021, p. 79–109.

6 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ L 277, 27.10.2022, p. 1–102.

A successful solution at national level

Poland, as a Member State responsible for protecting the European Union's external borders and having experience of the weaponisation of migration, has developed a national solution focused on countering online migrant smuggling, which works well.

A specialised cyber department has been created within the Polish Border Guard. Its main activity is to supervise and provide support to teams and organisational units of the Border Guard in the performance of tasks in the areas of cyber reconnaissance and criminal operational analysis during preparatory proceedings and where operational records indicate that a case may involve a cross-border element or multiple strands, may be especially complex, may involve a high degree of specialisation or may be connected to or develop organised crime.

DELETED

Questions

1) What do you see as the main challenges in countering migrant smuggling by the ever increasing use of digital means?

2) What tools and solutions should be developed, and which existing ones should be enhanced to support countermeasures against online migrant smuggling more effectively?

3) Do you see an added value in establishing counter-smuggling (particularly migrant smuggling) cyber intelligence units in each Member State and connecting them to Europol?