Council of the European Union

Brussels, 28 January 2025
(OR. en)

5556/25

LIMITE

ENFOPOL 21
CRIMORG 11
CT 9
CYBER 27
TELECOM 19
JAI 78

NOTE

From:	Presidency
To:	Delegations
Subject:	Use of prepaid cards to commit terrorist and criminal offenses

We would kindly ask delegations to respond to the questions set out in the attached document. The discussion paper will serve as a basis for the discussion following the presentation by the Polish National Expert. Please submit your **written replies by 3 March 2025**.

Furthermore, we would like to inform you that the Polish Presidency has conducted a comprehensive analysis of the issues related to Member States (MS)' regulations on access to prepaid SIM cards. Through the Secure Information Exchange Application (SIENA No 2382274-1-1), we have distributed questionnaires on the above-mentioned topic to Member States and other countries.

It is our intention to formalise the conclusions of the discussion on prepaid SIM cards in a Presidency report that will take into account the presentation and exchange of views of 23 January, as well as the written replies to this discussion paper and to the questionnaire sent through SIENA.

Introduction

Prepaid SIM cards are used for basic communications services such as calling, sending SMS messages and using the internet via mobile data. Buying a SIM card does not involve signing any subscription commitment or contract with an operator. The user purchases credits upfront and these can be used for communications services. Prepaid SIM cards are widely available in shops such as supermarkets or petrol stations and are one of the cheapest options for using phone services.

The issue of access to prepaid SIM cards is not regulated at EU level. This means that in some MS there are no restrictions on the purchase of prepaid SIM cards and they do not need to be linked to a payment card, identification document or passport. Some states have made it mandatory to register SIM cards. This means that an identity card must be presented when purchasing prepaid SIM cards. In this way, each SIM card purchased is linked to a user, making it much easier to monitor and identify mobile and internet accounts that require a telephone number.

The lack of harmonised rules on the mandatory registration of SIM cards in the European Union leads to differences in regulation between Member States. Some countries require SIM cards to be registered with the user's personal details, while others allow them to be purchased without restriction. As a result, criminals can anonymously purchase SIM cards from Member States without the required registration and use them throughout the EU.

Threats

The main threat associated with prepaid SIM cards is anonymity, particularly as there is no requirement to register the card with personal information, which makes it difficult for law enforcement agencies to monitor users and attribute activity to a specific person. As a result, prepaid SIM cards have become a tool for criminal activity and pose a real threat to public safety. In an era of rapid technological development, criminals are turning to encrypted instant messaging services such as Signal, Telegram, WhatsApp or Wickr, which offer end-to-end encryption and sometimes automatic message deletion features, so-called 'disappearing messages'. There is also widespread use of specialised encrypted networks such as EncroChat, Sky ECC or Phantom Secure, which not only offer strong encryption but also additional anonymisation features, such as a 'kill switch' that can be used to remotely destroy the contents of the phone. However, prepaid SIM cards are still an important element of communication between criminals. A phone number is often required to create an account on encrypted instant messaging services, and unrestricted access to prepaid SIM cards makes this type of communication much easier to access.

Cybercrime

Prepaid SIM cards play an important role in cybercrime, allowing criminals to conduct their online activities anonymously. Criminals can use them to create fake accounts on online platforms, register numbers for two-step verification or initiate scams such as phishing or spamming. These cards are also used to commit financial fraud via fake SMS or impersonating financial institutions. In addition, anonymous phone numbers are used on the darknet to contact cyber criminals and conduct illegal transactions. Prepaid SIM cards allow criminals to avoid detection and protect their activities from law enforcement, making them a key tool in the world of cybercrime.

Challenges

- **Anonymity of users:** the lack of mandatory SIM card registration makes it more difficult to associate a phone number with a specific person, allowing criminals to operate anonymously.
- **Barriers to communication traceability:** the inability to identify users makes it difficult to monitor criminal activities such as drug trafficking, fraud or terrorism**.**
- **Short-term use of SIM cards:** criminals use SIM cards on a one-off basis, making long-term tracking and evidence collection difficult.
- **Lack of international standardisation:** different countries have different SIM card registration regulations, allowing criminals to use cards purchased in Member States with less restrictive laws.
- **Exploitation in cybercrime:** registered SIM cards are used to set up fake online accounts, facilitating phishing, fraud and other forms of cybercrime.
- **Investigation costs:** the inability to quickly identify users increases the cost of operational activities such as monitoring or analysing telecommunications data.
- **Technological challenges:** criminals use registered SIM cards in combination with advanced technologies such as encryption, making it even more difficult to intercept communications.
- **Impeded prevention:** the inability to monitor and identify suspects makes it difficult to prevent crimes at the planning stage.

Questions to delegations

1. In your experience, do criminals and organised crime groups use unregistered prepaid SIM cards in their activities?

2. Are measures to monitor and identify individuals using unregistered prepaid SIM cards sufficient?

3. Have you noticed a high number of false alarms, e.g. bomb threats, from unregistered prepaid SIM cards?

4. Do you support the harmonisation of European regulations on mandatory registration of prepaid SIM cards at the time of purchase?