BANCA D'ITALIA
EUROSISTEMA

Supervisory Operational or Security Incident Reporting Framework

Horizontal Analysis 2024

June 2025

BANCA D'ITALIA
EUROSISTEMA

Supervisory Operational or Security Incident Reporting Framework

Horizontal Analysis 2024

June 2025

The work has been authored by Luca Cusmano, Valentina Cappa, Fulvio Di Stefano and Giulia Arangio.

The data presented are collected exclusively for supervisory purposes and are processed in aggregate form in compliance with privacy legislation.

The authors would like to thank the incident management team of the Statistical and IT Support Division, the management of the Directorate of Supervisory Institutional Relations, and the management of the Directorate General for Financial Supervision and Regulation.

Address
Via Nazionale 91
00184 Rome - Italy

Website
http://www.bancaditalia.it

Graphics by the Publishing and Printing Division of the Bank of Italy

TABLE OF CONTENTS

1. Introduction

This report summarizes the main findings from the reports of 'major operational or security incidents'[1] submitted in 2024 by intermediaries to Banca d'Italia, in accordance with the provisions of Circular No. 285, the Supervisory Provisions for Payment Institutions (PIs) and Electronic Money Institutions (EMIs), and the operational guidelines made available on the Bank's website.[2] The reports are collected within an incident reporting framework managed by the Directorate General for Financial Supervision and Regulation.[3]

In 2024, Banca d'Italia received 188 notifications of major operational or security incidents, a significant increase compared with those received in 2023 (approximately 45 per cent more). Key trends include a general rise in the number of notifications over the period, with a predominance of operational incidents (79 per cent of the total), a high level of involvement from external service providers (65 per cent of total notifications), and a slight increase in the number of cyber incidents (+8 per cent).[4] For the latter, Distributed Denial of Service (DDoS) attacks, which were the most common type in 2023, decreased. The economic impact of incidents remains limited, even though it increased compared with previous years. In a few cases, impacts exceeded €2 million. Service availability impacts are also rising, as shown by longer recovery times.

The following sections of the report provide further detail on the evidence from the incidents reported: Chapter 2 outlines the main trends observed in 2024, with a focus on causes (section 2.1) and impacts and resolution timelines (section 2.2), while Chapter 3 presents the main conclusions.

---

1 The regulation defines an operational or security incident as "any event, or series of related events, not planned by the bank that has, or is likely to have, a negative impact on the integrity, availability, confidentiality, and/or authenticity of services".

2 The framework applies to banks (including branches of non-EU banks), payment institutions (PIs), and electronic money institutions (EMIs).

3 2024 marks the last year in which the above-mentioned reporting framework for major operational or security incidents remained in force; it has been aligned with EU Regulation 2022/2554 (Digital Operational Resilience Act - DORA) since 17 January, 2025, as referenced in Banca d'Italia's communication dated December 27, 2024 (for further details, see the Banca d'Italia website: Reporting of major ICT-related incidents and voluntary notification of significant cyber threats https://www.bancaditalia.it/compiti/vigilanza/dora-incidenti/index.html?com.dotmarketing.htmlpage.language=1).The DORA framework extends the reporting obligations to new financial entities (e.g. investment firms, managers of alternative investment funds, management companies, crypto-asset service providers, issuers of asset-referenced tokens, and crowdfunding service providers), and introduces a new type of reporting, on a voluntary basis, for significant cyber threats.

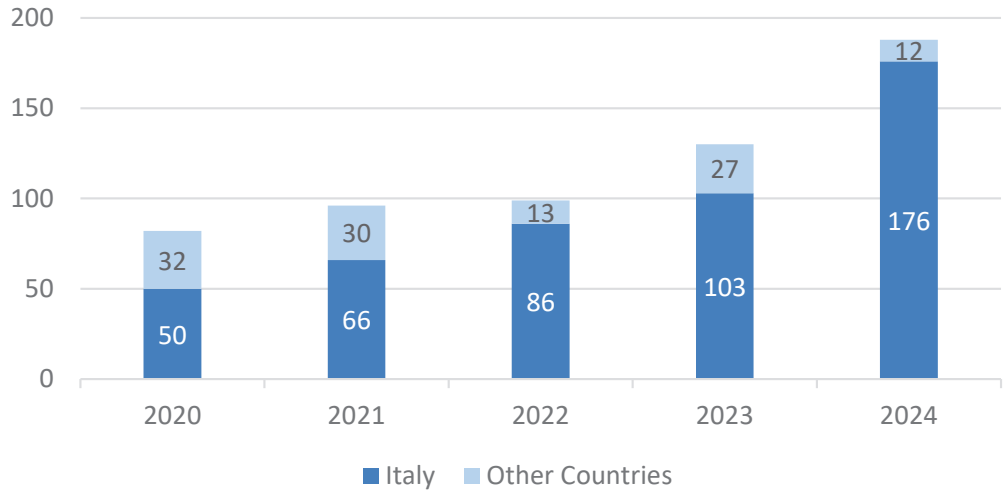
4 The main trends identified for the period 2020-2023 are therefore confirmed, as outlined in the analysis paper published by Banca d'Italia *'Digital resilience in the Italian financial sector: evidence from the supervisory incident reporting framework'* (https://www.bancaditalia.it/media/notizia/digital-resilience-in-the-italian-financial-sector-banca-d-italia-s-analysis-paper/?com.dotmarketing.htmlpage.language=1).

2. Evidence

The number of reports of major operational or security incidents received in 2024 has increased significantly compared with previous years (188 compared with 130 in 2023 and 99 in 2022 – see Figure 1).[5] The number of events reported[6] (103) has decreased slightly compared with 2023 (113), indicating that the individual events impacted more intermediaries on average.

Figure 1

INDIDENT REPORTS BY RELEVANT JURISDICTION (1)



(1) The total number of reports includes those from the foreign subsidiaries of Italian groups.

The 188 notifications were reported by 73 distinct intermediaries, which represent 47 per cent of all supervised intermediaries within the scope of the framework. The number of reporting entities has therefore increased significantly.[7] However, it is noted that 29 intermediaries (approximately 40 per cent) only reported one incident during the year.

Among the incidents reported in 2024, operational incidents account for about 79 per cent of the total (see Figure 2), showing a sharp increase compared with 2023 (148 with respect to 93, +59 per cent). The cyber incidents reported in 2024 – about 21 per cent of all reports – have increased slightly compared with the previous year (40 with respect to 37, +8 per cent). As in 2023, cyber incidents are mainly reported by significant banks, compared with less significant banks and other operators (see Figure 3).

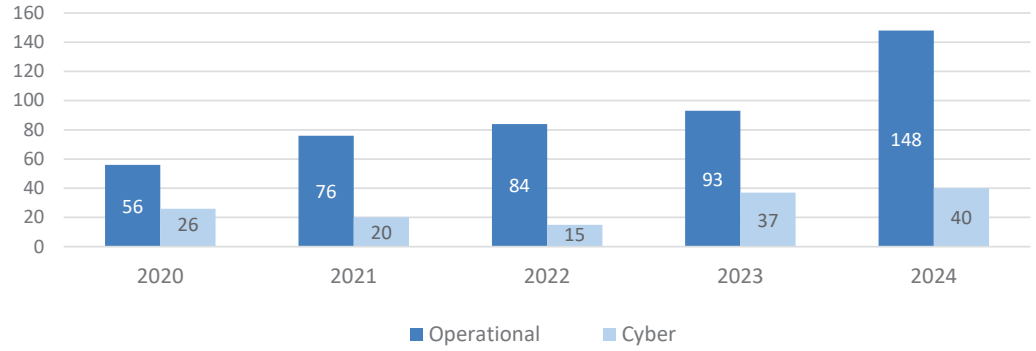
5 After an increase in the number of incident reports impacting the foreign subsidiaries of Italian groups in 2023, a new decrease in such cases was observed in 2024.

6 This refers to the individual events that impacted multiple intermediaries.

7 The percentage of reporters was 12 per cent in 2020, 19 per cent in 2021, 29 per cent in 2022, and 26 per cent in 2023.

Figure 2

INCIDENTS REPORTED BY CLASSIFICATION (OPERATIONAL VS CYBER)

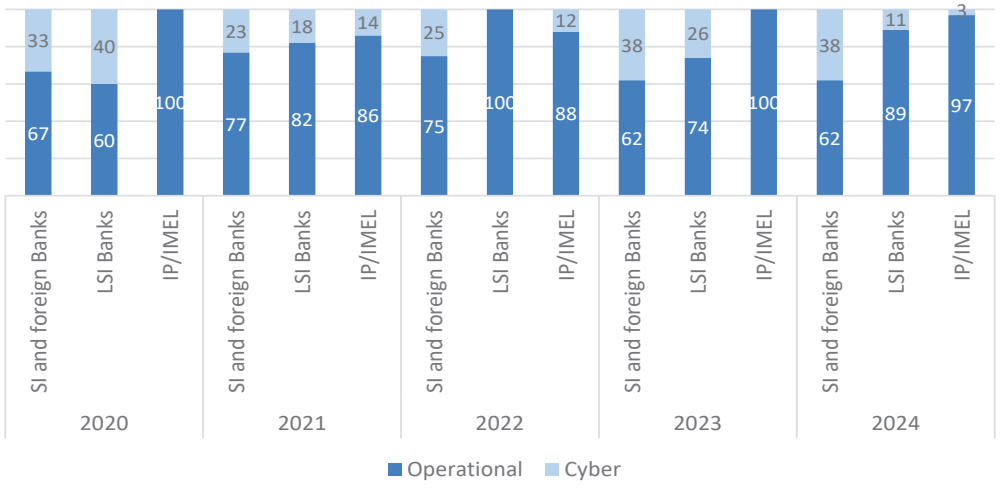


% / Year	2020	2021	2022	2023	2024
Operational	68%	79%	85%	72%	79%
Cyber	32%	21%	15%	28%	21%

Figure 3

INCIDENT CLASSIFICATION (OPERATIONAL VS CYBER) BY INTERMEDIARY CATEGORY

(percentage values)



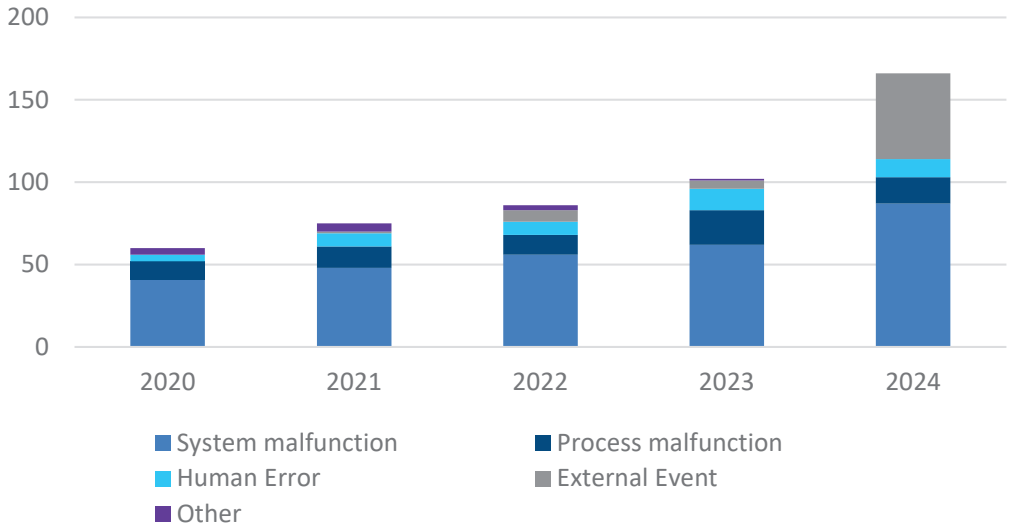
2.1 Root causes of the incidents

Operational incidents

The main cause of operational incidents, in line with previous years, is malfunctions, primarily relating to software issues and to a lesser extent to hardware problems, followed by human errors and process errors (see Figure 4). Operational incidents caused by IT changes accounted for approximately 30 per cent of total operational incident notifications.

Figure 4

OPERATIONAL INCIDENTS REPORTED BY TYPE

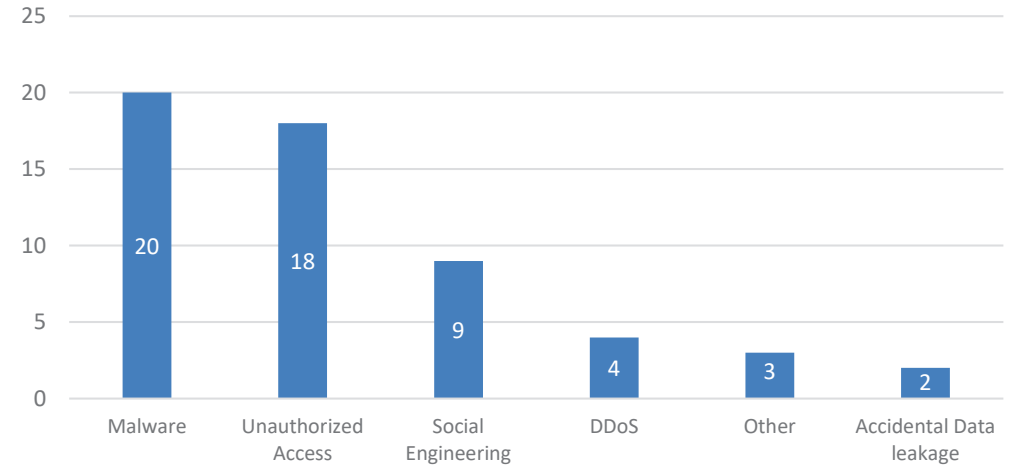


Cyber incidents

The 40 cyber incident reports received by Banca d'Italia in 2024 (compared with 37 in 2023, +8 per cent) originated from 30 distinct events, referring to 28 cyber-attacks and 2 accidental data leakages. In 2024, a significant decrease in DDoS attacks was observed compared with the previous year (from 16 in 2023 to 4 in 2024, -75 per cent), while all other types of attacks increased, including malware attacks, which also encompass ransomware, attacks carried out through unauthorized access, and social engineering attacks (see Figure 5).

Figure 5

CYBER INCIDENTS REPORTED BY TYPE – YEAR 2024



Throughout the year, the Bank conducted a detailed analysis of the cyber incidents reported by intermediaries between January 2023 and May 2024. The findings revealed that most of the cyber-attacks could be linked to known threat actors and, in some cases, the cyber-attacks caused significant economic impacts, particularly following malware and social engineering attacks that directly affected the intermediaries.

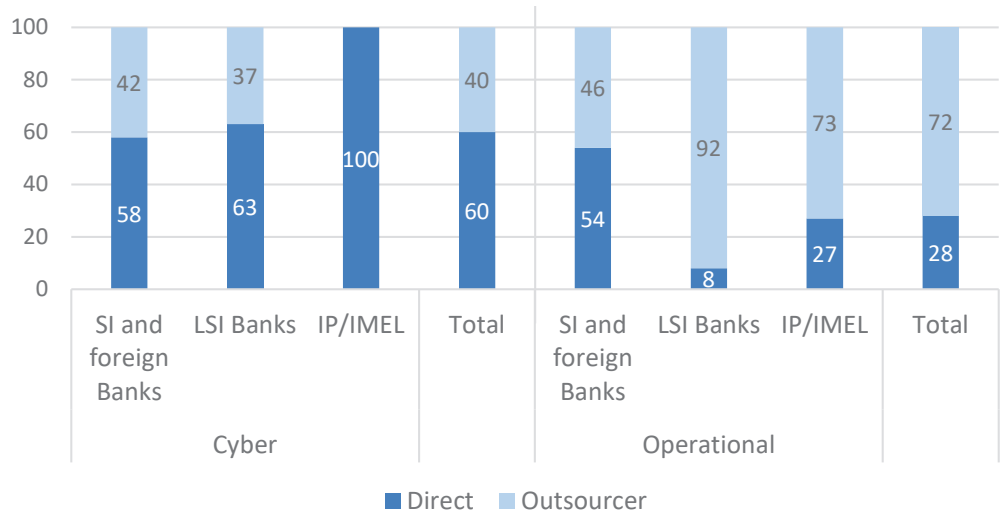
Involvement of service providers

A service provider was involved in 65 per cent of the reported incidents, with a higher involvement in operational incidents with respect to cyber incidents; this figure increased compared with 2023 (around 45 per cent). The incident originated in the service provider for most of the operational incidents reported by less significant banks, PIs and EMIs (see Figure 6).

Figure 6

RESPONSIBILITY BY CLASSIFICATION AND CATEGORY OF INTERMEDIARIES – YEAR 2024

(percentage values)



The high number of incidents involving a service provider confirms that the interconnection between various market players is a risk for intermediaries, as issues with third parties outside the supervisory perimeter can have an impact on supervised entities.

2.2 Impacts of incidents and resolution timelines

Most incidents (approximately 80 per cent) involved payment services (ATMs, web and mobile banking, wholesale payments, and so on) in 2024 too, with a percentage in line with previous years (see Figure 7). Payment services continue to be primarily affected by operational incidents (see Figure 8).

Figure 7

REPORTS WITH IMPACT ON PAYMENT SERVICES

(percentage values)

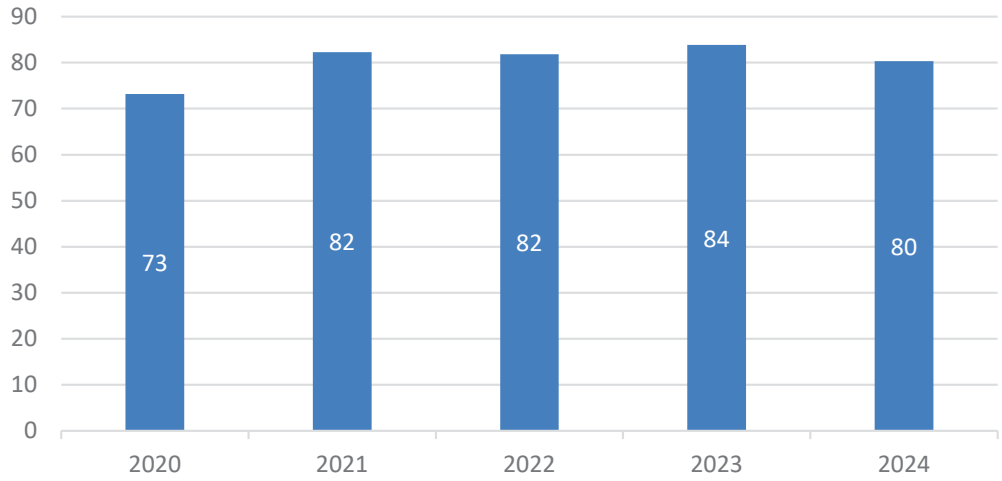
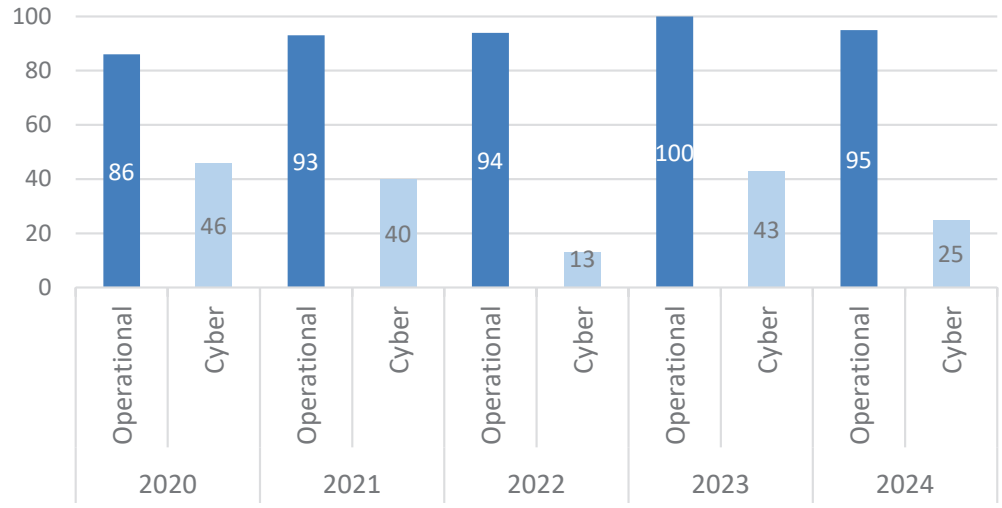


Figure 8

REPORTS WITH IMPACT ON PAYMENT SERVICES BY CLASSIFICATION

(percentage values)



The interruption of the availability and continuity of services is the main consequence of incidents and characterizes all types of intermediaries. Overall, about 70 per cent of all incidents resulted in the interruption of a service (whether payments, core banking, or ancillary services). Specifically, these incidents caused an average of about 21 hours of service disruption, a significant increase compared with 9 hours in 2023, mainly due to operational events relating to service providers. At the same time,

incidents that impact critical services[8] and a significant number of customers[9] (22 per cent of the total 188 reported incidents) have a lower average recovery time (about 13 hours), although it increased with respect to 2023 (about 5 hours).

The economic impacts[10] of incidents are, in most cases, not significant. However, in a few cases (7 out of 188), there was an economic impact greater than €2 million, particularly following social engineering attacks targeting the senior management of intermediaries, malware attacks on intermediary systems, erroneous IT changes, or operational errors.

8 Time-sensitive services are considered relevant, such as online banking, ATMs, and so on.

9 i.e. potentially affecting over 100,000 customers.

10 Within the incident reporting framework, economic impact refers to the total amount of losses, both direct and indirect, expressed in euros. Costs to be considered include, by way of example, hardware and/or software replacement costs, fines for non-compliance with contractual obligations, lost revenues, and so on. It is often difficult to quantify the economic losses accurately immediately following the detection of the incident and the intermediary therefore provides rough estimates. In subsequent updates of the incident, these estimates are gradually refined, but in some cases, the actual quantification of losses may occur long after the incident is closed, or may not occur at all (for example, in relation to potential legal expenses, lost revenues due to missed business opportunities, and so on.).

3. Conclusions

The operational or security incident reporting framework remains one of the most effective supervisory tools for monitoring and analysing the operational risk of supervised intermediaries and their service providers. It is a valuable tool for the timely assessment of system trends regarding new threats and vulnerabilities common to the Italian financial market.

The evidence gathered in 2024 shows that:

- the total number of incidents reported in 2024 increased significantly compared with the previous year (+45 per cent), although the number of individual events to which these incidents refer decreased (-9 per cent), indicating that individual events impacted more intermediaries, on average;
- the vast majority of reports concern operational incidents (79 per cent of the total), although the cyber incidents reported in 2024 slightly increased compared to the previous year (+8 per cent);
- a service provider was involved in 65 per cent of the reported incidents (compared with about 45 per cent in 2023), with a higher involvement i) for operational incidents compared with cyber incidents (where 72 and 40 per cent, respectively, involved a provider) and ii) for less significant banks (86 per cent), PIs and EMIs (71 per cent) compared with significant banks (44 per cent);
- in line with previous years, the main cause of operational incidents was malfunctions, primarily relating to software issues; in addition, operational incidents caused by IT changes accounted for about 30 per cent of the total;
- regarding cyber incidents, there was a decrease in DDoS attacks compared with the previous year, while all other types of attacks increased, including malware attacks, which also encompass ransomware, attacks carried out through unauthorized access, and social engineering attacks;
- incidents impacting the availability of critical services and a significant number of customers account for 22 per cent of the total and are primarily linked to operational incidents occurring at service providers;
- economic impacts of incidents are typically not significant; however, 7 reports indicated an economic impact exceeding €2 million.

The main risks highlighted in the analyses presented here are also confirmed by studies from the European Union Agency for Cybersecurity (ENISA)[11] and the ECB,[12] which identify ransomware attacks as one of the main threats at European level, including for the banking sector. At the same time, the compromising of

11 See ENISA, *Threat Landscape* 2024.

12 See ECB, *Evolving IT and cybersecurity risks*, November 2024.

corporate emails through social engineering attacks is reported as one of the main fraud techniques, according to studies by EUROPOL.[13] Among the main differences, it emerges that DDoS attacks remained numerous at the European level, while data from the reports show a decrease in such incidents.

The year 2024 marks the last year in which Banca d'Italia's incident reporting framework was active, as the new reporting scheme relating to the DORA regulation has come into effect starting from January 17, 2025. Incident reporting is one of the main pillars of the new regulation, requiring near real-time reporting and strong coordination processes between European and national authorities, for example through the immediate transmission of reports received by the ECB from significant banks, or the information sharing of incident reported in one Member State with impacts in other States. Banca d'Italia has started to receive the first reports of incidents in other European countries with a potential impact in Italy, the first reports from new entities previously excluded from the framework, and the first voluntary notifications of significant cyber threats from market operators. These elements will provide the opportunity to improve supervisory analyses both at the microprudential and macroprudential levels, allowing for the identification of risks relating to the innovative technologies to be dealt with various categories of intermediaries.

13 See EUROPOL, *Internet Organised Crime Threat Assessment* 2024.