




EGMONT GROUP
OF FINANCIAL INTELLIGENCE UNITS

Information Exchange Working Group (IEWG)

MAY 2023

USE OF OPEN SOURCE IN FIUS' OPERATIONAL & STRATEGIC ANALYSIS

Public Summary

TABLE OF CONTENTS

Overview/Executive Summary

The Egmont Group's (EG) Information Exchange Working Group (IEWG) initiated the "Use of Open-Source Intelligence in Financial Intelligence Units (FIUs) Operational and Strategic Analysis" project to assess the extent to which open-source intelligence (OSINT) affects or influences operational and strategic analysis. The project also aimed to identify the best practices through which FIUs identify reliable data sources and develop a list of the most consulted sources of information. A mixed methods approach was adopted, and qualitative and quantitative questionnaires were administered with responses from sixty-one (61) FIUs. Thematic and descriptive statistical analyses were used to analyze the qualitative and quantitative data, respectively.

Most notably, ninety-two (92) % of the study participants affirmed using OSINT for operational and strategic purposes. For operational purposes, OSINT is used mainly to get supporting information about the subjects of intelligence analysis and their transactions. OSINT is also used to identify subjects' networks, profile the subjects, identify adverse information about subjects, trace assets, and act as a trigger for new cases. For strategic analysis, OSINT mainly identifies money laundering/Terrorist Financing (ML/TF) trends and typologies. It is also used to identify factors influencing the effectiveness of anti-money laundering/counter-financing of terrorism (AML/CFT) regimes. The nexus between OSINT and financial intelligence (FININT) use during analysis were categorized into three (3) approaches:

1. **OSINT post-FININT**: This is the most common approach to combining OSINT and FININT data. With this approach, FIUs consult OSINT sources to support, corroborate, further develop and/or verify information from FININT analysis.
2. **OSINT pre-FININT**: In this approach, OSINT is used to raise suspicious transaction reports (STRs), which lead to FININT for further analysis.
3. **OSINT intra-FININT**: With this approach, OSINT is used during FININT, and both sources of information are intertwined.

Although a majority of the FIUs considered OSINT as beneficial in intelligence generation, some challenges were observed, which include the difficulty in verifying the source and information reliability, lack of required technology, subscription cost, jurisdictional/cross-jurisdictional internet prohibition and blockades, FIUs' specific internet content access prohibition, OSINT searcher anonymity concerns (non-tipping off the FIU interest), Data protection regulations/Data security laws, and information overload.

Different member countries suggested possible solutions to these challenges in their responses, including establishing an OSINT support team that will ensure safe information retrieval on open-source platforms (especially social media), the reliability of OSINT sources and data, and ensuring the effective management, analysis, and analysis use of the OSINT data.

These are the most common responses from member countries that did not specify the level at which this solution could be employed.

The use of OSINT for operational and strategic analysis has proven to have many positive advantages from the results of the survey returned by the FIUs. Regarding using OSINT around operational and strategic analysis, the FIUs indicated that OSINT contributes to various areas and is highly important. Among them is the development of typologies, the possibility of identifying patterns at a macro level, the possibility of identifying threats and trends related to money laundering and terrorist financing, links between

individuals and/or legal entities that cannot be identified in a suspicious transaction report (STR) but are related to other activities, positive/negative information on individuals or entities, among others.

1.0 Introduction

The questionnaire comprised five (5) sections with multiple-choice options, allowing the project team to generate easy-to-analyze data, provide mutually exclusive choices, and free entry text. These sections include:

1. **The use of OSINT for operational and strategic analysis**
2. **Types of OSINT used by FIUs**
3. **Development of databases, solutions, and tools for OSINT by the FIUs**
4. **Drawbacks and challenges of using OSINT in operational and strategic analysis**
5. **Case Studies/typologies on the use of OSINT in operational and strategic analysis**

2.0 Lay of the Land

This section presents an overview of OSINT use in FIUs as drawn from the data provided by participating FIUs. The findings in the section are categorized and explained as follows:

- **Number of FIUs that use OSINT**
- **How OSINT is utilized**
- **How OSINT and FININT are compiled**
- **Types of OSINT used**
- **Methods used to determine OSINT reliability**
- **Availability of dedicated OSINT teams and the development of OSINT tools**

2.1 Number of FIUs that Use OSINT

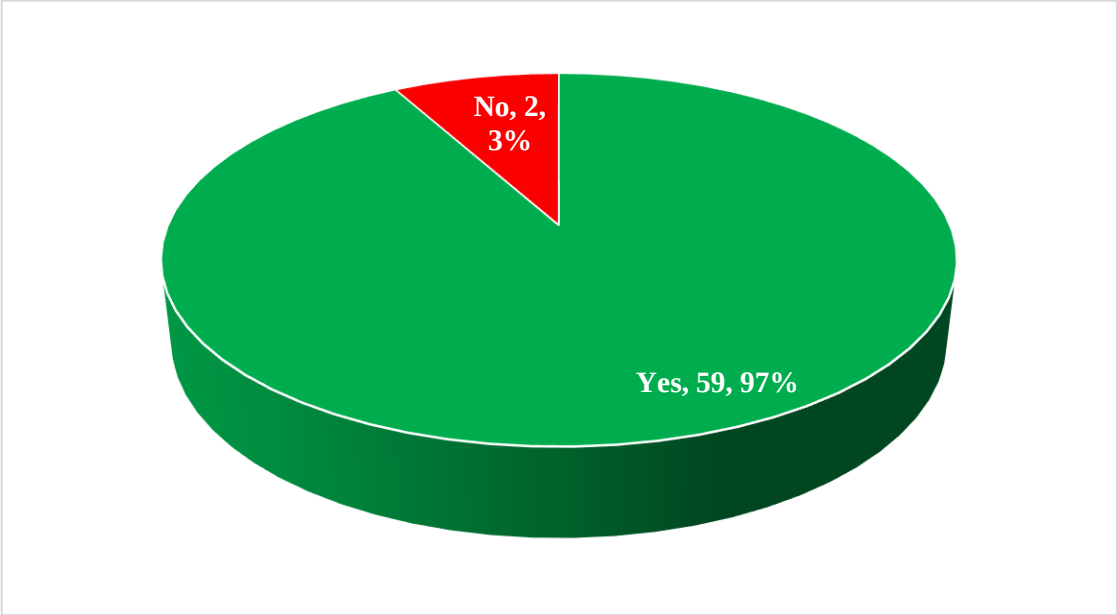

Figure 1: Responses on the Use of OSINT for Operational and Strategic Analysis

2.2 The Purpose of OSINT Usage in Operational and Strategic Analysis

Based on the responses from participating FIUs, some themes emerged to explain why OSINT is used in operational and strategic analysis. These are discussed in the following subsections.

2.2.1 Purpose of Usage in Operational Analysis

- **To get any available information about the subjects that will support ongoing financial intelligence analyses:** This is the principal reason for the participating FIUs' OSINT usage in operational analysis. OSINT use for information gathering here is not specific/targeted – the FIUs gather as much OSINT data as possible to help with their analysis.
- **To identify subjects' networks:** This is another common use of OSINT. Here, it is used to identify previously unknown subjects' connections, possible beneficiaries, and their activities.
- **To profile subjects:** OSINT is also used to ascertain the nature and characteristics of entities of interest and their activities.
- **To identify adverse information about subjects:** FIUs use OSINT to search for and gather adverse information about entities of interest.
- **For asset tracking:** OSINT could detect financial activities and asset tracing, including real estate, luxury goods, etc.
- **As a trigger for new FIU cases**: OSINT data have initiated new FIU cases independently and not just as a supporting information source for ongoing cases.

2.2.2 Purpose of Usage in Strategic Analysis

- **To identify ML/TF trends and typologies:** Most participating FIUs reported using OSINT in strategic analysis to identify ML/TF threats, materiality, and context and to model adequate mitigations and controls accordingly.
- **To identify factors that influence the effectiveness of AML/CFT regimes:** FIUs reported that OSINT is used in strategic analysis to study other countries' AML/CFT policies and identify factors that influence their effectiveness.

2.3 Types of Open-Source Intelligence for Operational and Strategic Analysis

This section presents the types of OSINT used by participating FIUs. These are categorized into domestic and international OSINT. Domestic OSINT refers to open sources of information within an FIU's jurisdiction, while international OSINT refers to information sources outside the FIU's jurisdiction.

2.3.1 Domestic OSINT

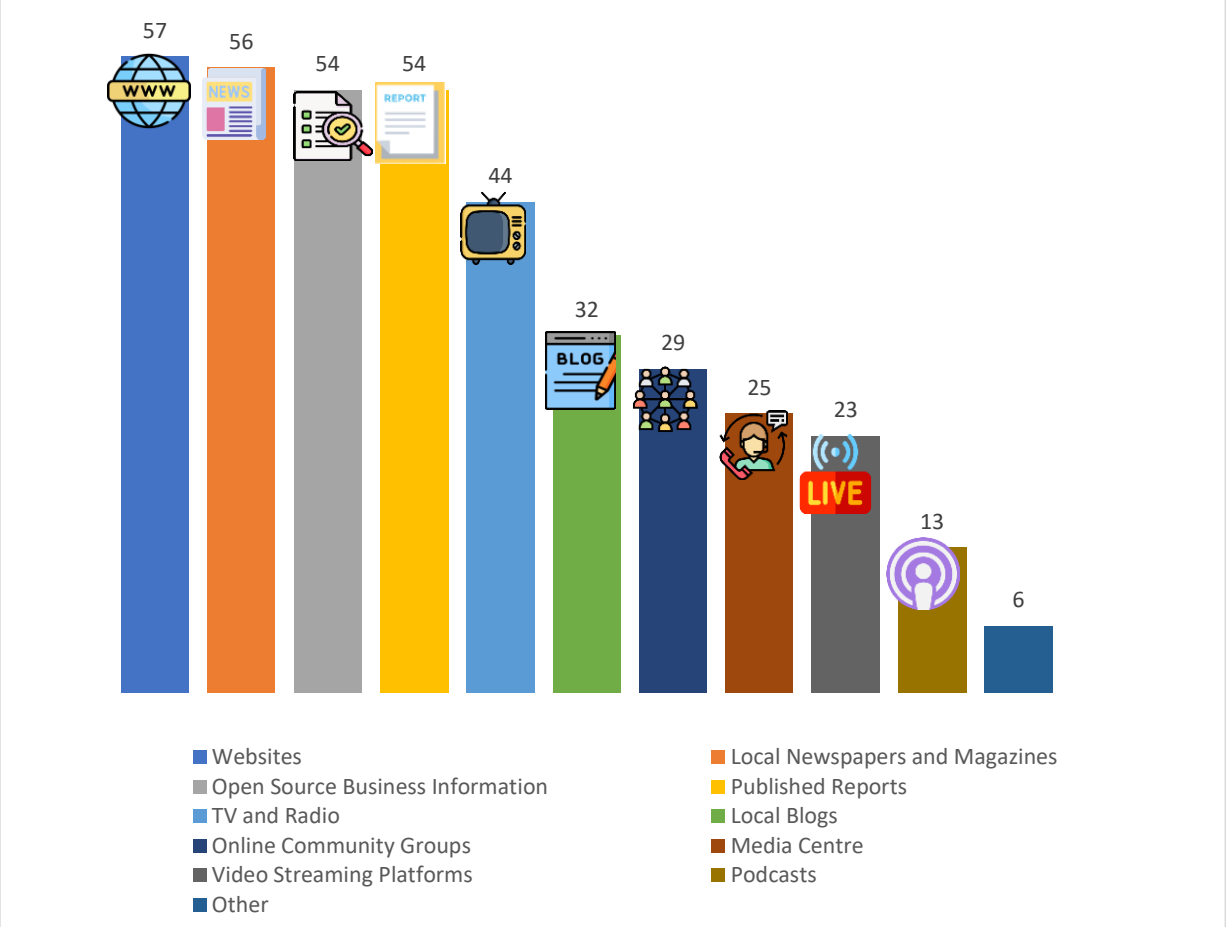

Figure 2: Domestic Open-Source Intelligence

Figure 2 reveals websites as the most popular type of OSINT used for analysis among FIUs (accounting for 93% of responding FIUs). This shows that most use domestic websites to obtain intelligence. Other

domestic sources of OSINT among the top five (5) include local newspapers and magazines, published external reports, open-source business information, and TV and radio, all selected by at least 70% of the responding FIUs. At the tail end, the bottom five (5) include podcasts, media centres, online community groups, video streaming platforms, and local blogs.

2.3.2 International OSINT

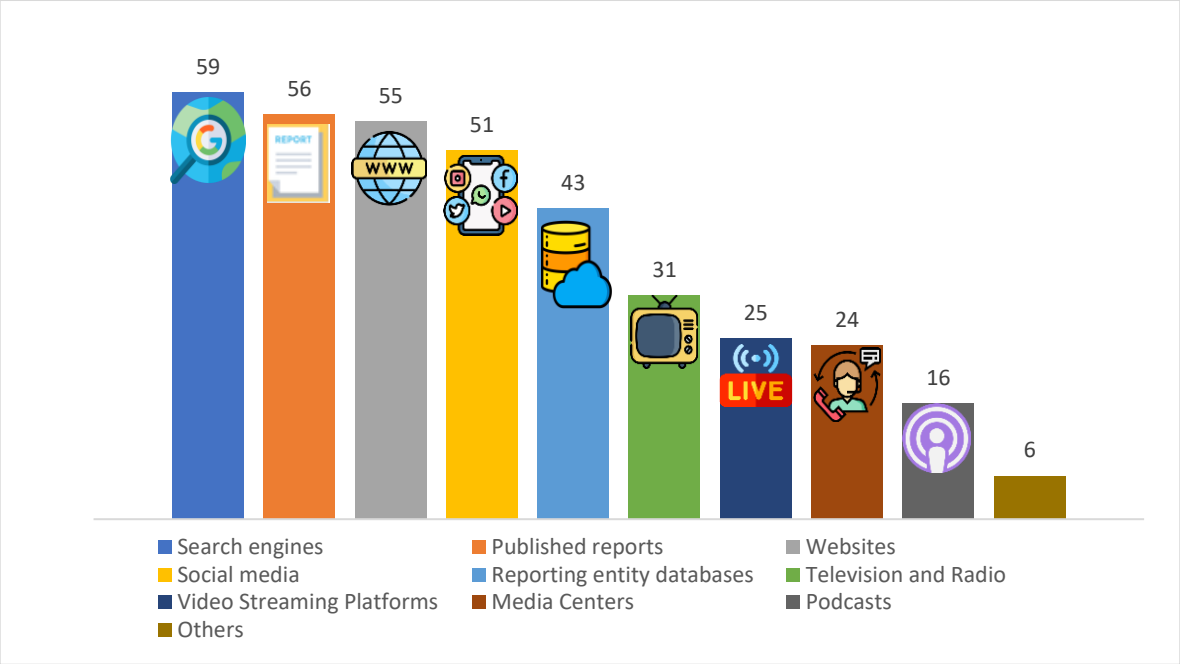

Figure 3: International Open-Source Intelligence

As shown in **Figure 3**, among fifty-nine (59) FIUs (accounting for 97% of responding FIUs) reported using search engines for OSINT, thus making it the most popular OSINT tool in use by FIUs. Search engines are popular around the world for both intelligence and non-intelligence analysts. Other international OSINT types in the top five (5) include published external reports, websites, social media, and reporting entities' databases. On the other end of the tail, the bottom four (4) include podcasts, media centres, video streaming platforms as well as TV and radio.

2.4 Reliable Sources of OSINT Used by FIUs

Participating FIUs provided links to reliable OSINT platforms used to generate intelligence reports. Fifty-eight (58) FIUs responded with multiple websites and pages they rely on as sources of OSINT. The most frequently mentioned among the responses are outlined below.

- **Search Engines**
- **Social Media**
- **Publicly available reporting entity databases**
- **Websites of other FIUs**
- **Local and Foreign official webpages**
- **Virtual Assets Websites**

2.5 The Use of Social Media OSINT for Operational and Strategic Analysis

This study specifically investigated FIUs' use of social media as a source of OSINT. Social media was singled out because of the ubiquity of social media platforms and because it is a significant source of OSINT. The results presented in **Figure 4** below indicate that fifty (50) FIUs, representing 82% of responding FIUs, use social media OSINT for operational and strategic analysis, while eleven (11) responded negatively.

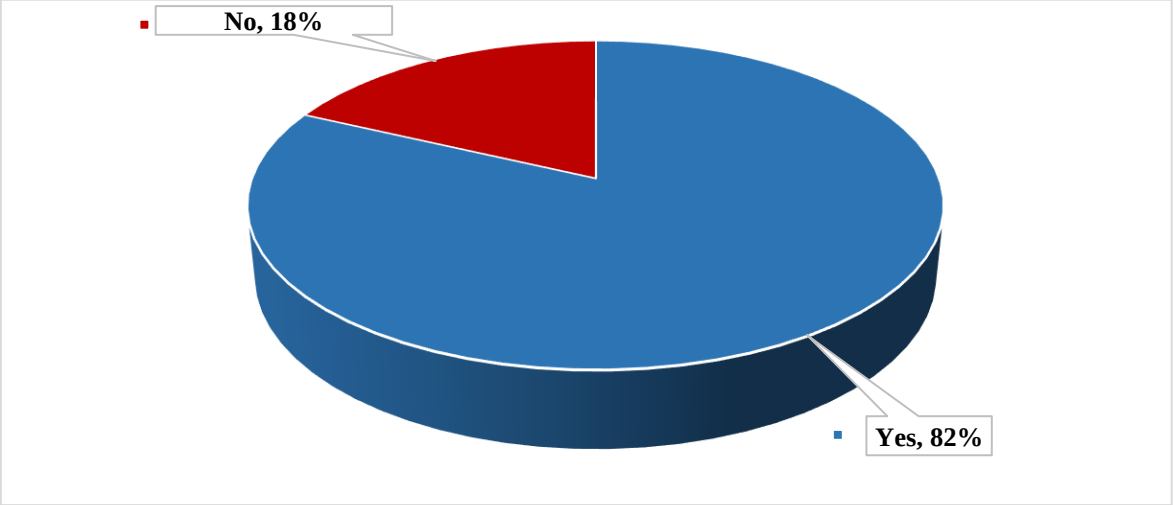

Figure 4: Responses on the Use of Social Media OSINT for Operational and Strategic Analysis

2.6 Methods and Strategies Used to Ensure OSINT Reliability

With regards to the reliability of the OSINT, most FIUs provided the methods and strategies they use to determine the reliability of their open-source information. This section presents the approaches adopted by FIUs in determining/ensuring reliable OSINT sources and data. They include (some of) the following:

- **Reliance on trusted media:** This is another common approach that FIUs adopt, using OSINT data only from reputable sources like news sites, official records or pages belonging to public authorities and international bodies, etc.
- **Crosschecking with multiple sources:** With this approach, FIUs determine reliability by crosschecking OSINT data with data from other sources, whether official or not. This approach can also indicate reliance on information spread, meaning that the more widespread an OSINT information piece is, the more reliable.
- **Source-information reliability checks:** FIUs also adopt some form of reliability assessment to gauge the reputation of their OSINT sources and the trustworthiness of their information.
- **Reliance on contents posted by an entity of interest or close associates:** With this approach, FIUs rely on information posted or provided by a subject of interest or close associates.
- **Subjective judgement**: The analysts should determine the reliability of OSINT sources, data, and information using the FIU's judgement.

2.7. Availability of Dedicated OSINT Teams and the Development of OSINT Tools

The section presents findings on the number of FIUs with dedicated teams/departments responsible for handling, managing, or analyzing OSINT data. Some (26%) of participating FIUs indicated they have dedicated teams, while most (74%) do not (**Figure 5**).

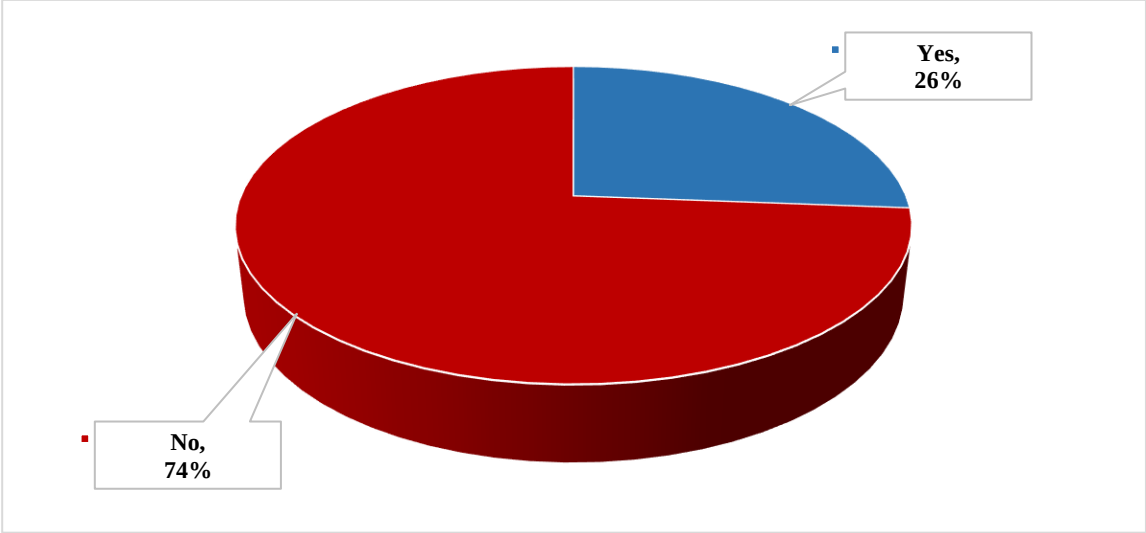

Figure 5: Availability of Dedicated OSINT Teams/Departments

The section also presents findings regarding the OSINT databases and tools developed and used by the FIUs. The majority (69%) of responding FIUs indicated the unavailability of an OSINT database accessible to analysts within their FIUs. The minority (31%) indicated otherwise (**Figure 6**).

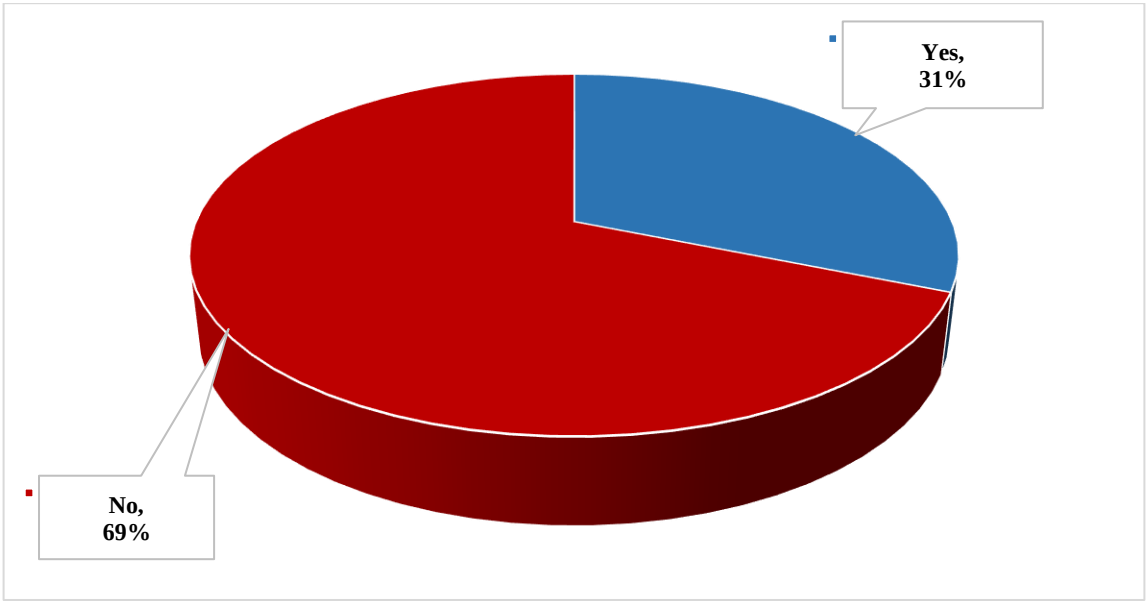

Figure 6: Development of OSINT Databases Accessible to FIU Analysts

Based on participating FIUs' responses, the tools are categorized as follows:

- **OSINT platform link/URL repository:** This is the most common tool for participating FIUs. It provides analysts with a list of OSINT platforms and hyperlinks. The analysts visit these platforms based on necessity during analysis.
- **OSINT platform monitoring solution:** This helps FIUs monitor OSINT platforms' content. One FIU reported its use.
- **OSINT platform content extractor**: This solution extracts/scrapes content from OSINT platforms.
- **Database of adverse media reports:** This solution collects and stores adverse media reports.
- **OSINT data archive:** This stores analyzed OSINT data and information that resulted in intelligence reports.
- **Subscription to OSINT platforms:** Some FIUs reported relying on OSINT platforms and tools they purchase or subscribe to.

2.8. Challenges of OSINT Use and the Way Forward

In this section, FIUs provide information on the drawbacks/challenges they experience using OSINT and the measures adopted to mitigate them. Insights on this are provided in the subsequent sections.

2.9. Types of OSINT Drawbacks/Challenges Faced by FIUs

From the chart below, "**potential information overload**" is the **most common challenge** (39%) faced among responding FIUs, alongside data security laws (17%) and legal impediments (13%).

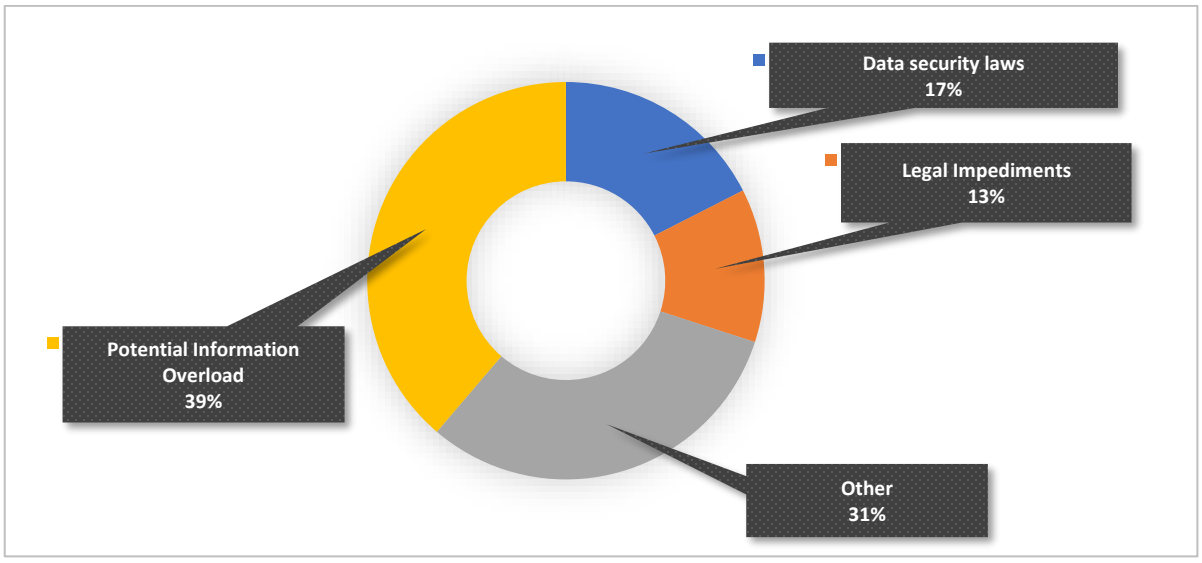

Figure 7: Drawbacks/Challenges Faced by FIUs in the Use of OSINT

Interestingly, some FIUs also face other challenges besides those listed. Their responses to this are presented below.

- **Difficulty verifying the source and information reliability:** This was the major challenge reported by participating FIUs.

- **Lack of required technology:** FIUs also highlighted challenges posed by the lack of technology to integrate open-source information into existing databases, facilitate the handling and processing of unstructured OSINT data, and facilitate the effective combination of OSINT and FININT data.
- **Subscription cost:** Some FIUs also find subscription costs for proprietary, open-source information platforms challenging.
- **Jurisdictional/cross-jurisdictional internet prohibition and blockades:** A government's decision to prevent citizens from accessing certain platforms can impede access to open-source information platforms. It can also be hindered if, due to diplomatic disputes, a foreign government prevents access to specific platforms by users from another country.
- **FIUs' specific internet content access prohibition:** Internet access and use policies implemented by FIUs may prohibit access to OSINT data sources.
- **OSINT searcher anonymity concerns**: There are also concerns about maintaining the anonymity of FIUs and staff while conducting OSINT on social media platforms.

3.0 Conclusion and Recommendations

3.1 Conclusions

Open-source intelligence derived from publicly available data and information was identified as an excellent resource for operational and strategic analysis and intelligence generation by FIUs. The study revealed that it is not limited to what can be found using Google, although the "surface web" is an essential component.

The use of OSINT for operational and strategic analysis has proven to have many positive advantages, according to the survey results of participating FIUs. The FIUs indicated that OSINT contributes to multiple areas and is highly important. Among these areas are the development of typologies, the possibility of identifying patterns at a macro level, the possibility of identifying threats and trends related to ML/TF, links between individuals and/or legal entities that cannot be identified in a suspicious transaction report (STR) but are related to other activities, positive/negative information on individuals or entities, among others. It is essential to mention that FIUs indicated that the most significant drawbacks or challenges of using OSINT in operational and strategic analysis are potential information overload, data security laws, and legal impediments to using OSINT.

However, as valuable as OSINT can be, information overload is a genuine concern. Some FIUs use different tools and techniques (including IT implementation) to conduct OSINT initiatives that address these challenges. The downside of OSINT, which FIUs need to be cognizant of, is that anything FIU Intelligence Analysts can find can also be found (and used) by preparators of predicate offences.

3.2 Recommendations

On this note, the following was recommended:

- FIUs must have a clear strategy and framework for using OSINT in operational and strategic analyses. FIUS must develop their OSINT capabilities and integrate these activities into its internal operations, including providing targeted training to FIU staff, most frequently using OSINT.

- While using OSINT, FIUs must closely consider several factors, such as information quality, source, and data reliability.
- When using OSINT, the data source has the minimum reliability characteristics, which implies that information may vary in accuracy and validity; therefore, critical evaluation is required. Also, vulnerabilities associated with using OSINT need to be considered while using them.
- Before deciding to use OSINT to strengthen the operational and strategic analysis, consider any contraindications, inconveniences, or challenges in each jurisdiction, such as legal impediments and data security laws, among others.
- Where possible, FIUs are encouraged to seek their domestic and international partners' (including foreign FIUs) confirmation/verification of the validity and reliability of the OSINT collected within their operational and strategic analysis.