IEWG

EGMONT GROUP

OF FINANCIAL INTELLIGENCE UNITS

- EGMONT GROUP PUBLIC BULLETIN -

FIU'S CAPABILITIES AND INVOLVEMENT IN THE FIGHT AGAINST THE FINANCING OF EXTREME RIGHT-WING TERRORISM: STATE OF PLAY AND PERSPECTIVES

JULY 2021

PUBLIC BULLETIN:

EXTREME RIGHT-WING TERRORISM FINANCING

The purpose of this bulletin is to present key lessons, best practices and representative case examples to help enhance the fight against extreme right-wing terrorism financing both at national and international levels. The information in this bulletin should assist the establishment of national strategies and facilitate effective cooperation between FIUs and law enforcement and with judicial authorities. It should also help reporting entities better detect extreme right-wing terrorism behaviours.

INTRODUCTION

According to a note published in April 2020 by the United Nations Counter-Terrorism Committee Executive Directorate (CTED)[1], research shows there has been a 320% rise in attacks conducted by individuals affiliated with extreme right-wing (ERW) movements and ideologies the previous five years.

Although lone actors and small cells have committed the majority of extreme right-wing terrorism (ERWT) attacks, the international community considers that, as the threat has increased, ERW groups and individuals are more often operating transnationally. According to the CTED, recent evidence suggests "there has been a greater exchange of views between like-minded individuals, both online and offline" and that these "connections would allow ERW groups to improve their tactics, develop better counter-intelligence techniques, solidify their violent extremist views and broaden their global networks."

In this context, financial intelligence units (FIU) have access to key information, albeit limited at this stage, which can indicate financing of ERWT. Moreover, the fact that this threat is increasingly transnational in nature warrants increased involvement from the FIU community. Indeed, FIUs use very efficient mechanisms to cooperate operationally, both domestically and internationally and can identify new links, patterns, and methods related to these terrorist activities and their financing through financial intelligence. FIUs may be able to provide relevant financial information that can be instrumental in identifying a person's involvement in ERW movements and their intent to commit violent actions.

FIUs indicate, however, a need for more background information and knowledge on the phenomena of ERW extremism and terrorism to be able to identify relevant money flows. This information may come from specialized competent authorities, such as law enforcement agencies (LEA) or intelligence services and be shared with the domestic FIU.

---

1 https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/cted_trends_alert_extreme_right-wing_terrorism.pdf

To understand the threat and to find the best ways to tackle them, the information exchange working group (IEWG) of the Egmont Group wrote a report aiming to identify the main challenges faced by FIUs when contributing to investigations of ERWT activity and offers best practices to enhance the effectiveness of FIUs in addressing ERWT threats. It provides an overview of how FIUs can make the best use of financial information and intelligence at the domestic level and cooperate with each other when considering this form of terrorist financing (TF). This report also intends to analyze the current state of play and highlight how FIUs can work to achieve better results in disrupting this specific kind of TF.
Although the analysis produced as part of this project recognizes that ERWTF is a subject not yet well understood by the private sector, the cases in this book illustrate that FIUs make most detections via suspicious transaction reports (STR) and suspicious activity reports (SAR) they received from reporting entities coupled with the use of specific financial indicators.

The analysis found that domestic authorities are taking this threat into account and that solutions are found for combating ERWTF, but some room for improvement exists.

Extreme right-wing terrorism

For the purpose of this project, extreme right-wing terrorism will be defined according to the definition used by UN CTED as far-right or racially or ethnically motivated terrorism.

Egmont Group contributors are also encouraged to refer to the following definition: "Right-wing terrorists seek to force political, social, and economic systems to follow an extremist right-wing model. A core concept in right-wing extremism is supremacism, the idea that a certain group of people sharing a common element (nation, race, culture, etc.) is superior to all others. Seeing themselves in a supreme position, the particular group considers it their natural right to rule over the rest of the population. Racist behaviour, authoritarianism, xenophobia, and hostility to immigration are commonly found attitudes in right-wing extremists. Right-wing terrorism refers to the use of terrorist violence by right-wing groups, such as neo-Nazi, neo-fascist, and ultranationalist formations".

KEY LESSONS AND BEST PRACTICES

- Reflecting on the ERWT risk at the domestic level with all involved parties to enable relevant stakeholders to:
    - Better understand the ERWT threat (which would facilitate the detection by both competent authorities and the private sector);
    - Better understand the capacities and legal capabilities of each involved party and their role in the fight against ERWT, which enhances the quality of investigations and avoids the duplication of effort.
    - Widen the scope of the national risk assessment (NRA) and, if needed, explicitly analyze the threat of ERWTF.
    - Consider the creation of a task force that will deal with TF or specifically with ERWTF, including FIUs.
    - Consider the role of the domestic FIU in the risk analysis of the threat at the domestic level, especially regarding the operational and strategic information sharing to leverage financial intelligence.

- LEAs should support the domestic FIU with a view to gain a better and common understanding of the groups and individuals involved at the domestic level, thereby strengthening FIU's analysis.
- Organize public-private information sharing. Whether focused on strategic analysis or operational information and if allowed by the national legislation, sharing information between the task force or the national coordination mechanism and relevant actors of the private sector is a way to raise awareness of such threats within the private sector. This may occur *via* a public-private partnership (PPP) or by scheduling periodic meetings between the parties to discuss relevant matters.
- The creation of risk indicators appears essential for the detection and investigation of ERW cases. Risk indicators can be designed by the FIUs, attested by competent authorities, or jointly created. Once completed, these indicator sets should be widely shared with competent authorities and reporting entities.

CASE EXAMPLES

1. Understanding ERW organizations through the analysis of their financial status and support networks

Description of the case:
The domestic FIU received a suspicious transaction report (STR) concerning Association A after its high-profile unlawful activities were reported in the media. The reporting entity suggested Association A was collecting funds for illegal purposes. The FIU analyzed Association A's financial activities and identified links to another violent ERW organization. Furthermore, the analysis identified that the Association had received donations from an alleged perpetrator of an ERW terrorist attack in Country Z. The FIU disseminated its findings concerning Association A to national security authorities based on suspected ERW activities.

Financial Analysis:
Following receipt of an STR, the FIU gathered information regarding Association A from open and closed source databases to which the FIU has direct access. Data used by the FIU included was contained in the national association register, tax authority database, bank account register and spontaneous disclosures from counterpart FIUs. This additional information enabled the FIU to conduct an in-depth analysis of Association A's activities. Through this analysis, the FIU was able to identify related persons of interest as well as domestic and foreign income streams to customer accounts held by the Association. Requests for further information to obtain account statements and KYC data were made to relevant domestic banks and foreign-based FINTECHs (via foreign FIU counterparts). Financial analysis revealed links to a violent ERW organization known for hate ideology and donations received from the alleged perpetrator of an ERW terrorist attack in Country Z.

Data overview:
(Alleged) offence
Collection of funds for illegal purposes.

Profile of suspect
A supposed non-violent ERW association attempts to elevate its public status through high-impact operations.

Financial products and transactions

Cheques, e-money transfers to foreign countries *via* FINTECH, international wire transfers and cash deposit/withdrawal.

Key factors in FIU's case handling

- Direct access to competent authorities' databases and the EU's cross-border reporting system was key to enabling the FIU to identify information and related entities of interest in a timely manner.
- The FIU's ability to use the bank account register to target relevant financial institutions and request further information was also key.
- The FIU leveraged spontaneous disclosures from its international network of FIUs to understand the financial activities of Association A and related persons of interest (POI) to request further information from foreign-based FINTECH entities.
- In the wake of a terrorist attack in Country Z, the FIU proactively checked publically disclosed information against its own data holdings and identified relevant transactions which were spontaneously disseminated to Country Z. This further demonstrates the FIU's effectiveness in handling the case.

Challenges

A primary challenge was the delayed access to information from a foreign FINTECH entity.
The process to request further information from reporting entities, triggered at several points in the case, also extended the time it took to complete the analysis.

Outcome/Results

The FIU's analysis supported competent domestic authorities and foreign FIUs to develop knowledge of ERW groups and their activities by mapping their financial supports.
Positive and detailed feedback from domestic LEAs regarding the analysis enabled the FIU to identify links to another network, which prompted further analytical work not covered by this case study.

2. Analysis of transactions of a suspect of ERW terrorist offences

Description of the case:
A person with ERW views was convicted for planning a terrorist attack on left-wing opinion-makers, politicians, and Muslim community targets. This person was illegally in possession of 1800 rounds of ammunition, 2 deactivated firearms and a recipe to build an Improvised Explosive Device (IED). The case was discovered when he approached an illegal weapon dealer to procure firearms.

In this case, STRs were reported but not related to terrorist activities. It did not add extra value to the burden of proof in the case but had added value for the intelligence position.

3. Analysis of transactions of an ERW group

Description of the case:
In 2020, the FIU received intelligence concerning a specific ERW group and its funding. Since the domestic Security Services recently had increased the national threat assessment of ERW, it was decided to find all available intelligence on ERW groups in the country and try to identify sources of funds and use of funds.

The analysis was primarily based on STRs and OSINT.

The main source of funding was identified as donations, either through bank transactions or by cryptocurrency. There were identified several cash-withdrawals concerning some ERW groups. The use of funds was identified primarily to be printing of the material to be used in activism and vandalism.

There were no identified links to buying of material that could be used for attacks or other illegal activity in the available financial intelligence.

4. Analysis of purchasing behaviour

Description of the case:
Using transaction data collected from reporting entities, the FIU analyzed purchasing behaviour of two POIs to establish trends and patterns over time. The FIU detected a change in transacting behaviour from purchases of ERW ideological items to more tactical items, assessed to possibly indicate an escalation in the security risk they presented. The two initial POIs also sent multiple payments to three alleged recruiters for an international ERW group. Through financial network analysis, the FIU discovered further eight more individuals sending funds to the offshore recruiters. A number of these additional POIs were found to have purchased multiple ideological and tactical items online, a further indicator of the group being of security interest. The number of payments sent to the recruiters indicated the POI's commitment to ERW ideology and the strength of the relationship between the POIs and recruiters.

5. Analysis of online purchases

Description of the case:
Proactive analysis of transaction data, in particular payment details collected from reporting entities, led the FIU to identify a POI assessed to have been inspired by an international attack event. Over a two-year period, the POI made several ERW memorabilia and iconography purchases – assessed to indicate ideological support – and tactical items, such as outdoor clothing and equipment. The FIU analyzed the POI's purchasing behaviour, established trends and patterns over time and observed that the purchases increased noticeably following the racially motivated attack. The FIU referred the POI to law enforcement partners for an investigation to determine whether he represented a threat to the community.

Differentiating between those who support a far right-wing (FRW) or ERW ideology from financial data can be challenging for FIUs, as individuals who align with the far-right often engage in activities that could resemble extremists planning an attack, including having an interest in weapons, gun ownership and purchasing tactical items associated with survivalist behaviour and 'prepping.' ERW online forums and groups promote ERW attackers such as the Christchurch and Halle attackers as 'saints' and models of how to undertake successful attacks. Therefore, iconography and tactical items consistent with a previous attacker may indicate a person of security relevance and a heightened risk for mobilizing to violence. Analysis to establish trends and transact patterns over time and purchases that seek to replicate items used in previous attacks can be used to identify individuals for further investigation.

6. Suspected money-laundering offence by a person linked to an ERW organization

Description of the case:
On 18.06.2019, a male person with a suitcase of cash (EUR 50,000 in small bills) appeared at the district court (depository). This man deposited a bail at the Local Court for his son, who is an officer of a special police force. The cash payment served as a so-called bail payment to suspend the arrested man's imprisonment after issuing a warrant.

As a result, the official in charge at the depository contacted the Ministry of Economics, Labour and Health because he could not rule out a possible suspicion of money laundering. On this occasion, the Ministry of Economics, Labour and Health issued a money laundering suspicion report.

The facts of the case are said to be connected to investigations against network A, a group of ERW, which is said to include, among other members of the Armed Forces and the police, the colleague mentioned above of the special force.

Network A was an association of ERW, soldiers and policemen accused of preparing for an expected state collapse on "Day X" and of having planned a subsequent mass killing of refugee aid workers and considered political opponents. The group was formed in early 2016 and became known in August 2017. Together with similar groups, it was part of the ERW network B that was discovered in 2018. In the case of network A, it was determined that data on individual persons, institutions or organizations were collected in a targeted and continuous manner within the framework of intensive research.

7. Terrorism – the assassination of a politician

Description of the case:
Suspicions were raised and provided to domestic FIU based on negative open-source media regarding three foreign citizens arrested for the fatal shooting of a PEP.

One of the main suspects, from a European Union (EU) country, an ERW individual, confessed to the killing soon after being arrested in mid-June 2019, which he recanted at the beginning of July 2019.

In addition, the subjects appeared to be mentioned in a compliance database, categorized as Nonconventional Terror (alleged Neo-Nazi, no known affiliation to any terrorist or militant group).

The reporting entity conducted a detailed financial analysis of all transactions done by the suspects over a period of almost three years and identified:

- sales and purchases of firearms components,
- car parts and,
- small payments from five individuals residing in three different EU Member States, without any explanation.

Those detected small incoming payments, without explanation, from other individuals located in various EU member states allowed to identify two further individuals who also purchased different firearms components.