



EXTREME RIGHT WING TERRORISM FINANCING PHASE II

Information Exchange Working Group

Abstract

The second Egmont Group report on the rise of extreme right wing (XRW) terrorist groups and associated terrorism financing addresses a number of limitations and challenges that the first report in 2022 identified by looking at ways to improve understanding and detection of XRWTF.

TABLE OF CONTENTS

Table of Contents.....	1
Glossary.....	1
XRWTF II – Public Summary.....	2
Indicators.....	2
Operational analysis.....	3
Blueprint.....	4

GLOSSARY

XRWTF	Extreme Right Wing Terrorism Financing
Egmont Group	Egmont Group of Financial Intelligence Units
FIUs	Financial Intelligence Units
XRW	Extreme Right Wing
STR	Suspicious Transaction Reports
RMVE	Religiously Motivated Violent Extremism
IMVE	Ideologically Motivated Violent Extremism
CT	Counter-Terrorism
FATF	Financial Action Task Force



XRWTF II – PUBLIC SUMMARY

This second Egmont Group report on the rise of extreme right wing (XRW) terrorist groups and associated terrorism financing addresses a number of limitations and challenges that the first report in 2022 identified. It looks at ways to improve understanding and detection of XRWTF, as well as explores the scope to move beyond bilateral exchange to engage multilaterally where possible on XRW threats. Both elements are examined mainly through an operational lens.

This phase II report covers four areas:

- ▶ an XRWTF threat update and project member country snapshots
- ▶ outcomes and lessons from testing a trial set of XRWTF indicators
- ▶ operational analysis of two major XRW groups and
- ▶ insights and lessons from joint operational analysis of a few cases, using a blueprint developed for that purpose.

A key overall finding is that XRW groups globally are only loosely connected and differ significantly from the main religiously motivated violent extremism (RMVE) groups and related TF risks. The global XRW movement lacks a coherent, unified ideology or narrative. Central groups or hubs (with linked network structures) do not exist to coordinate or provide strategic direction to the XRW groups and cells scattered across the globe, despite the fitful efforts of some actors to become more centralised. The fragmented nature of the XRW threat poses challenges for FIUs (and intelligence/law enforcement agencies) and reporting entities in detecting and responding to XRWTF actors and activity.

INDICATORS

To support FIUs develop and apply XRWTF indicators in practice, project members tested a large set of indicators against their own data holdings. While this proved to be a challenging exercise, it yielded valuable lessons to support FIUs to develop useable indicators. The report provides better practice measures for FIUs to employ, as well as suggestions to address technical challenges in using indicators to detect XRWTF.

The list of indicators includes three tiers of terms which can be used to both identify new cases and aid practitioners with interpreting information during their analyses. Each tier is weighted according to the level of an individual's knowledge of, or affinity and association with, XRW/IMVE. As with general indicator methods, combining indicators across the tiers can help assess the level of risk associated with an individual or network, or provide useful contextual information.

The loose, eclectic nature of XRW/IMVE ideology, reflected in the niche terminology of different groups, makes it challenging to produce a broad set of indicators for international use. To provide operational value, XRWTF indicators need to be carefully aligned and calibrated for specific XRW/IMVE groups operating in jurisdictions or (sub) regions.



OPERATIONAL ANALYSIS

The analysis of two major XRW groups also identified several indicators associated with financial activity, particularly for training, recruitment, and propaganda. One of the groups that were assessed concerns accelerationist neo-Nazis. Accelerationists derive their ideology from a range of sources. These include James Mason’s neo-Nazi SIEGE, the satanist Order of Nine Angles, and ‘a plethora of terrorists and fringe texts’. Such ideological works are shared via social media.¹

The project team assessed financial intelligence related to both accelerationist facilitators and attackers. The available intelligence suggests that these types of actors engage in some distinct activities and appear to have differing financial indicators as well. Whereas the attackers engage in attacks and attack plots, the facilitators engage in activities as summed up in Figure 1:

Activities
<ul style="list-style-type: none"> - Flexible combination of on- and offline activities - Instigation of terrorist violence - Conducting concealed communications - Engaging in international travel - Connecting international like-minded individuals

Figure 1. Activities of accelerationist neo-Nazi facilitators

These activities entail their own financial indicators. On the one hand, the facilitators received and used their funds in the following ways:

Source of funds	Use of funds
<ul style="list-style-type: none"> - Government benefits - Sale of merchandise - Sale of clothing - Sale of propaganda 	<ul style="list-style-type: none"> - webhosting - payments to producers of merchandise, clothing, propaganda - international travel

Figure 2. Accelerationist neo-Nazi facilitators’ finances

Whilst receiving and spending the funds, the accelerationists deployed a variety of payment methods. Some of their activities occur on openly available social media, which are free-of-use, do not require payments and thus are unlikely to leave a money trail.

On the other hand, the project team identified the following indicators for accelerationist attackers:

Phase	Indicator
Preparation for (a potential) attack	Ideological indicators <ul style="list-style-type: none"> - purchase of right wing and neo-Nazi clothes - purchase of Nazi literature - purchase of Nazi and Soviet military goods - transactions to likeminded individuals Operational indicators <ul style="list-style-type: none"> - online contacts with likeminded individuals - purchase of weapons and ammunition

¹ <https://www.isdglobal.org/explainers/the-order-of-nine-angles-explainer>;
<https://www.bbc.com/news/world-53141759>;
<https://www.splcenter.org/hatewatch/2018/02/22/atomwaffen-and-siege-parallax-how-one-neo-nazi%E2%80%99s-life%E2%80%99s-work-fueling-younger-generation>

	<ul style="list-style-type: none"> - activities at military locations - training related transactions
Pre-attack indicators	<ul style="list-style-type: none"> - travel related transactions - account dormancy

Figure 3. Financial and behavioral indicators for Accelerationist neo-Nazi attackers

As a note for the public, we would like to stress that the above-mentioned indicators were established in post-event analyses. The occurrence of one or more of these indicators doesn't have to indicate terrorist activities and, without additional information, may relate to legitimate activities. As seen with the indicators model, a tiered approach using indicators weighted according to likely levels of violent extremist ideology, attack preparation and capability purchases should improve detection results.

BLUEPRINT

To promote collaboration on transnational threats, the project team designed a blueprint to guide joint operational work and tested it against a few select cases. Sharing operational data on a multilateral basis helped identify relevant individuals/persons of interest and their activities, map out previously unknown branches of networks, and substantiate typologies. Analysts meeting face to face enabled wider analytical techniques to be applied to the data, produced deeper insights than usually occurs through formal bilateral exchanges, and proved a faster way to exchange information. This pilot work and its associated blueprint provides a basis for similar multilateral exchanges to be pursued on other threat financing themes. It also provides a test case for the Egmont Group to consider for developing a multilateral exchange framework, drawing on the findings of any further joint projects that may follow.





EGMONT GROUP

OF FINANCIAL INTELLIGENCE UNITS

WWW.EGMONTGROUP.ORG

The goal of the Egmont Group of Financial Intelligence Units (Egmont Group) is to provide a forum for financial intelligence units (FIUs) around the world to improve co-operation in the fight against money laundering and the financing of terrorism and to foster the implementation of domestic programs in this field.

The IEWG builds opportunities for FIUs to share operational intelligence, develop technical solutions for effective information exchange, and work collaboratively to address emerging ML/TF risks and vulnerabilities.