Targets of Terrorgram
The Who, What, and Where of Threatening Communication on Terrorgram.

Lukas Lundmark[1], Antonia Hamich Andersson[1], Lisa Kaati[1], and Katie Cohen[2]

[1] Stockholm University, Stockholm, Sweden
firstname.lastname@dsv.su.se
[2] Swedish Defence Research Agency (FOI), Sweden
{katie.cohen}@foi.se

Abstract. This study analyzes propaganda from the Terrorgram Collective, a decentralized far-right network of Telegram channels and users that promote violent accelerationism. Drawing from three key Terrorgram publications disseminated between 2021 and 2023, 393 instances of threatening communication have been extracted and analyzed. The threats are categorized along four analytical dimensions: type (general violence vs. specific plans), mode of communication (direct, indirect, veiled), target type (soft vs. hard), and target group. The analysis suggests that threats in Terrorgram publications are mainly directed at soft targets — i.e., individuals and minority communities —and primarily communicated through veiled or indirect language. Moreover, threatening communication in Terrorgram publications frequently includes operational guidance designed to encourage lone-actor violence.

Keywords: Terrorgram · Violent accelerationism · Telegram · Digital propaganda · Far-right extremism · Threat detection

1 Introduction

On 9 September 2024, the US Department of Justice announced the indictment of two individuals accused of exploiting the encrypted messaging platform Telegram to incite hate crimes, promote the assassination of federal officials, and conspire to provide material support to terrorist organizations [15]. According to the indictment, the defendants held influential positions within the so-called Terrorgram Collective, a loosely affiliated constellation of Telegram channels and users dedicated to the dissemination of violent accelerationist content.

The indictment further states that the indicted individuals had distributed a variety of multimedia materials containing explicit instructions to carry out acts of violence. Aside from glorification of previous lone-actor offenders, the material also included the dissemination of a so-called "kill list", identifying high-profile targets, including government officials at the federal, state, and local levels, as well as corporate executives and leaders of nongovernmental organizations. Many

of those named were allegedly selected based on characteristics such as race, religion, national origin, sexual orientation, or gender identity.

The Terrorgram Collective (hereafter referred to as Terrorgram) has become a central node in the militant accelerationist sphere, operating solely through Telegram. This network is notorious for distributing violent propaganda and encouraging acts of lone-actor terrorism, aiming to disrupt democratic societies [2,1]. On Terrorgram, users collaborate to create a narrative that justifies and even necessitates extremist violence as a means to protect "White" people from perceived enslavement and extermination by "the System" [18].

The goal of this study is to analyze threatening communication in Terrorgram publications and categorize the threats along four analytical dimensions: type (general violence vs. specific plans), mode of communication (direct, indirect, veiled), target type (soft vs. hard), and target group. The analysis aims to uncover how threats are used to incite violence against various targets in order to advance the ideological objectives of militant accelerationism.

2 Terrorgram Publications

A prevalent mode of communication within Terrorgram is the production and circulation of so-called *zines*—digitally formatted magazines that integrate text and imagery within deliberately designed layouts. The zines are highly effective propaganda instruments, in part because the interplay of visual and textual elements can elicit a stronger persuasive effect than text alone [8]. The magazine format enables the presentation of more extensive and thematically cohesive content, thereby fostering an impression of ideological sophistication that is less readily conveyed through shorter forms of media such as memes. Digital zines are highly accessible: they can be easily downloaded, shared, and archived, enhancing their reach and longevity compared to typical social media posts or memes.

Terrorgram zines exhibit striking similarities to the violent manifestos produced by individual attackers [10]. The zines often follow a recognizable narrative structure, where they typically open with a crisis-oriented exposition that frames the world as being under existential threat, assigning blame to perceived enemies such as minority communities or governmental institutions. This is usually followed by an ideological rationale that draws on extremist, mainly white supremacist and accelerationist, doctrines to legitimize the use of violence. Many zines also include tactical material, offering detailed instructions or strategic advice on how to conduct attacks or create disruption, similar to operational content found in manifestos such as those authored by the perpetrators of the Christchurch and Buffalo shootings. The zines often conclude with an explicit call to action, urging readers to join the struggle and carry out further acts of violence.

The exact number of Terrorgram zines is unknown due to its decentralized media production. In this study, we have analysed three key zines shared on Telegram between 2021 and 2023: Militant Accelerationism: A Collective Handbook

(Part 1), Do it for the Gram, and The Hard Reset: A Terrorgram Publication (Parts 1–5).

3 Method

To facilitate the analysis of the Terrorgram zines, textual content from each page was initially extracted using optical character recognition (OCR). To identify threatening communication, we trained a machine learning model using two different datasets. The first dataset was created by [5] and further described in [4] and employed in [16] to train various classifiers for threat detection. The second dataset is described in [14] and [9]. For our model, we combined these two datasets, resulting in a training set consisting of 2,151 texts labeled as threatening communication and 26,432 texts labeled as non-threatening. We used a pretrained RoBERTa model from HuggingFace's transformer library[3] as the base. For training, we randomly partitioned our dataset into a training (85%), validation (5%), and test split (10%). The model was trained for ten epochs, using a batch size of eight, with an Adam optimizer [6] with a learning rate set at $5e-6$. The max sequence length was set to 256 tokens. The experiment was rerun multiple times and test results (accuracy, precision, recall, and F1-score metrics) on the model with the highest accuracy on the validation set. The performance of the model is shown in Table 1.

Table 1. Performance metrics of the RoBERTa-based classifier used to detect threatening communication, showing precision, recall, F1-score, and support for both threatful and non-threatful categories.

	Precision	**Recall**	**F1-Score**	**Support**
Not threatful	0.99	0.98	0.98	1326
Threatful	0.76	0.83	0.79	113
Accuracy			0.97	1439
Macro Avg.	0.87	0.9	0.89	1439
Weight Avg.	0.97	0.97	0.97	1439

3.1 Analyzing Threats

All text segments extracted from the zines were processed using the trained classifier. Segments flagged as potentially threatening were then subjected to manual annotation, guided by four analytical categories designed to capture key characteristics of the threats:

1. **Type of threat** – Differentiates between explicit threats that include concrete instructions or detailed plans, and more generalized statements that imply a willingness to commit violence without specifying actions.

[3] https://huggingface.co

2. **Mode of communication** – Categorizes the threat as direct, indirect, or veiled, based on how openly and explicitly the intent to cause harm is conveyed.
3. **Soft/Hard target** – Indicates whether the threat is aimed at a soft target (e.g., individuals, communities, or vulnerable groups) or a hard target (e.g., critical infrastructure, government buildings, or security forces).
4. **Target group** – Identifies the specific person(s), group(s), or entity that is the intended recipient of the threat.

3.2 Type of Threat

Each threat was categorized into two broad types:

- **General Violence:** Threatening communication that implies violence but lacks specificity regarding the target or method of attack. The communication lacks concrete details about targets, methods, or timing, and are often used to express ideological support for violent action or to foster a general climate of intimidation.
- **Specific Instructions/Plans:** Threatening communication that explicitly outlines an illegal activity or provides detailed instructions on how to carry out such acts. These threats contain operational details such as the identity of intended targets, specific attack methods, tactical advice, or step-by-step plans.

The categorization enables a clear distinction between general rhetorical violence and more actionable threats, which is essential for informing both analytical interpretations and practical responses by practitioners. While rhetorical violence can contribute to radicalization and the normalization of extremist ideologies, actionable threats (those that contain specific plans or instructions) demand immediate attention due to their significantly higher potential to result in real-world harm.

3.3 Mode of communication

Each threat was further categorized based on its mode of communication, following the framework proposed by O'Toole [12]. This categorization captures how explicitly or implicitly the intent to cause harm is conveyed, which is important when assessing the immediacy and clarity of the threat. The three categories are as follows:

- **Direct Threat:** A threat in which both a specific act of violence and a specific target are clearly identified. Such threats leave little room for interpretation and explicitly state what the perpetrator intends to do and to whom. For example: "I am going to do (specific act) to (specific target)."
- **Indirect Threat:** A threat that is more ambiguous, offering no clear commitment to act or specific identification of a target. It suggests that violence could occur but leaves significant uncertainty about whether, how, or against whom it would be carried out. For example: "If I wanted to, I could..."

– **Veiled Threat:** A threat that subtly implies the possibility of harm, often relying on context or inference by the recipient to understand the message's threatening nature. Veiled threats create a sense of unease or intimidation without making an explicit reference to violence or an illegal act. For example: "We would be better off without you," or "I know where you live" [13].

3.4 Soft/Hard Targets

The target of each threat was classified as either a **soft** or **hard** target. Soft targets are defined as human beings, either as individuals or as members of an identifiable social group, regardless of their level of protection or vulnerability to attack. The categories considered soft targets include: Authorities, Ethnic and Religious Groups, LGBTQ and Individuals and Collectives. In contrast, hard targets are defined as locations, buildings, or systems, such as government offices, military installations, or police facilities.

3.5 Target groups

For each threat, the target group was identified and categorized. The identified target groups include:

– **Authorities:** Government officials, law enforcement, political leaders, and representatives of state power.
– **Ethnic and Religious Groups:** Ethnic and religious minorities, as well as groups targeted for their beliefs or backgrounds, including those labeled by Terrorgram as "race traitors".
– **LGBTQ:** Lesbian, Gay, Bisexual, Transgender, and Queer individuals or communities, often targeted for their sexual orientation or gender identity.
– **Individuals and Collectives:** A broad category encompassing both individuals (e.g., a single person) and collectives (e.g., crowds, communities, or movements).
– **Transport, Power, and General Infrastructure:** Includes transport networks (e.g., cars, railways, roads) and critical infrastructure such as power grids, gas stations, and communication systems.
– **Societal Institutions:** Public and private spaces such as schools, hospitals, police stations, government buildings, and other institutions central to societal functioning.
– **The System:** Refers to broader societal structures, including political, economic, and legal systems that maintain social order and stability.

4 Results

A total of 393 threats were identified across the analyzed Terrorgram publications. Approximately 78% of the identified threats fell into two main categories: General Violence and Specific Instructions/Plans. The majority (66%) were classified as General Violence—threats that imply violent intent without specifying a

target or method—serving primarily to intimidate and normalize violence. The remaining 34% were categorized as Specific Instructions/Plans, providing explicit guidance on whom to attack and how. These operational details highlight the propaganda's tactical intent and closely mirror the strategies used by groups like the Islamic State (IS), which similarly disseminate step-by-step instructions for violent acts. This resemblance suggests that Terrorgram employs comparable ideological and strategic mechanisms in its efforts to incite violence.

The second dimension of the analysis focused on the mode of communication used in the threatening content. Among the identified threats, 75% (n=292) were categorized as either direct, indirect, or veiled, reflecting varying degrees of explicitness and ambiguity. Figure 1 shows the distribution of the different modes of communication in the threats. In summary, 23% of the threats were categorized as direct, 20% as indirect, and 31% as veiled threats.

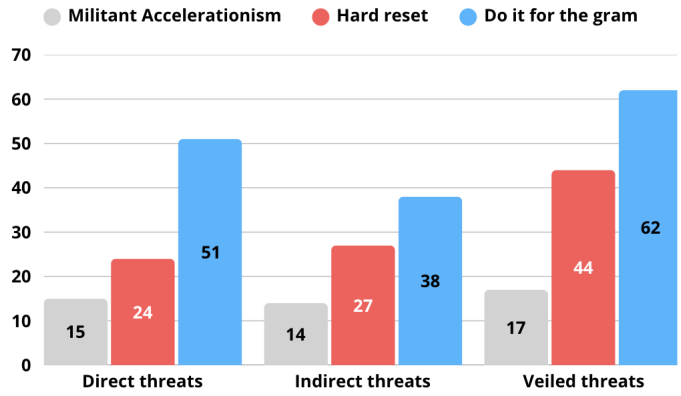

Fig. 1. Distribution of threats by mode of communication (direct, indirect, veiled) across the three analyzed Terrorgram zines illustrating the prevalence of implicit and ambiguous forms of threatening language.

The third dimension of the analysis examined whether the threat was directed at a soft or hard target. Of the 393 threats identified, 76% (299) included a clearly specified target. Among these, 65% were aimed at soft targets, which encompassed categories such as authorities, ethnic and religious groups, LGBTQ+ individuals, and broader social collectives. The remaining 35% were directed toward hard targets, including power infrastructure, transportation systems, societal institutions, and abstract entities referred to as The System. // The fourth dimension focused on the specific target group of each threat. Fig. 2 displays the number of threats directed towards a specific target group. *Individuals and Collectives*, are the most frequently targeted group, followed by *Ethnic and Religious Groups*, and then *Power, Transportation, and General Infrastructure.*

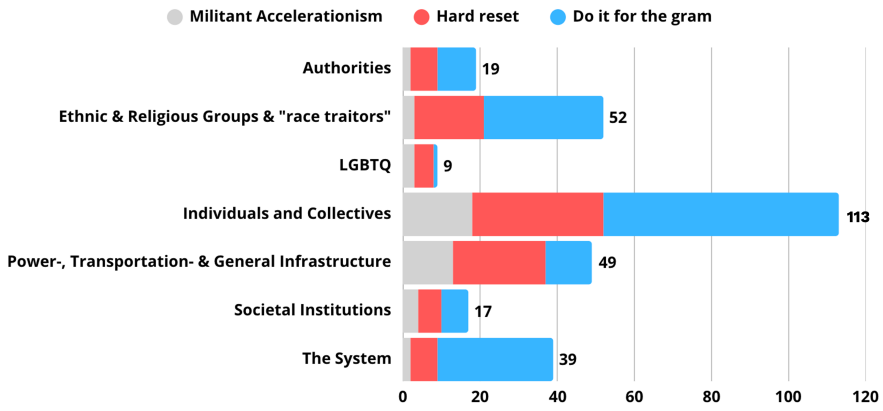

Fig. 2. Number of threats directed at each target group in the analyzed Terrorgram zines.

5 Discussion

Most of the identified threats (66%) fall under the category of General Violence, meaning they imply a violent intent without offering specific operational details or explicit targeting guidance. These threats serve primarily to create an atmosphere of fear and to normalize the idea of violence as a legitimate political tool. They also contribute to the construction of a broad, ideologically charged narrative that frames violence as both inevitable and necessary. In contrast, 34% of the threats provide Specific Instructions or Plans. These threats go beyond rhetorical posturing by offering detailed guidance on whom to attack and how to execute such acts. The presence of these operational messages aligns with a broader trend in extremist propaganda, where strategic communication is used to inspire and enable attacks. This tactic closely mirrors the well-documented communication practices of jihadist groups such as the Islamic State (IS), which has long used similar methods to foster lone-actor attacks and decentralized forms of terrorism [17].

The mode of communication is another critical dimension. A significant portion of the threats are conveyed using veiled or indirect language (together constituting a large share of the messages), rather than straightforward direct threats. This technique serves multiple purposes: it provides plausible deniability for the propagandists, increases the psychological impact on potential targets by introducing uncertainty, and can have a stronger mobilizing effect on susceptible individuals by allowing them to project their own interpretations onto the messages.

The empirical analysis indicates that the majority of threats identified in the selected Terrorgram publications (65%) are directed toward soft targets.

Although comprising a smaller proportion, threats directed at hard targets (35%)—including critical infrastructure, societal institutions, and "The System"—reflect the movement's militant accelerationist objective of provoking systemic collapse. These threats underline Terrorgram's alignment with broader accelerationist goals, where destabilization of the state and its institutions is a central aspiration.

Within the soft target category, *Individuals and Collectives* constitutes the largest subgroup, accounting for 38% of all threats. This high figure is explained by the prevalence of ambiguous references such as "they," "them," or "he" in this category. The lack of contextual information in many extracts likely contributed to this classification.

The second largest soft target category is *Ethnic and Religious Groups*. As detailed in Section 4.1 of the study, the ideological foundation of Terrorgram is based on the belief that the "Aryan race must come first." Accordingly, threats directed at ethnic and religious minorities mirror the in-group/out-group antagonism that the ideology is centered around. Thus, threats toward ethnic and religious groups also serve to symbolically reinforce the collective identity of the imagined white community. A key feature of Terrorgram propaganda is its deliberate construction of a cohesive group identity. This identity formation relies on fostering a shared sense of belonging and purpose, often rooted in extremist ideologies such as white supremacy and militant accelerationism [7].

The category *LGBTQ+* comprises 3% of the identified threats. Previous research demonstrates that far-right ideologies are often intertwined with hostility and violence toward non-normative sexual and gender identities [3]. Such hostility is often rooted in beliefs linking family regulation and reproduction to national and racial purity. Far-right groups perceive LGBTQ+ identities as threats to these ideals. Some scholars interpret this hostility as a reaction to societal changes, while others attribute it to long-standing ideologies such as racism and xenophobia. Murib [11] noted that the notion of "gender ideology" is often politically weaponized to scapegoat LGBTQ+ individuals while promoting white supremacy and rigid gender norms.

Finally, 6% of the threats are directed at authorities, such as law enforcement and other representatives of the state. This aligns with the ideology of the Terrorgram Collective, a militant accelerationist movement seeking societal collapse through violence. Attacking authorities, such as police, is consistent with the goal of disrupting societal order and law enforcement structures.

Notably, the propaganda strategies employed by Terrorgram share significant structural and functional similarities with those of the Islamic State (IS). Both entities utilize digital media to amplify their ideologies, recruit sympathizers, and incite acts of violence. They both encourage lone-actor attacks, providing ideological justification alongside practical instructions. While IS frequently promotes attacks using easily accessible weapons such as vehicles and knives, Terrorgram publications often advocate for the use of homemade explosives and firearms.

These similarities demonstrate a convergence in strategies among extremist groups across ideological divides, leveraging digital platforms and psychologically targeted messaging to radicalize individuals and incite violence.

6 Conclusions and Directions for Future Work

This study offers new insights into the communicative strategies of the Terrorgram Collective through an analysis of 393 threats across four analytical dimensions: type of threat, mode of communication, target type, and target group. The results of the analysis demonstrate that Terrorgram publications are not merely conveying an ideology, but also act as operational tools aimed at fostering radicalization and inciting violence.

The findings reveal that a substantial majority of threats are directed at soft targets, with Individuals and Collectives and Ethnic and Religious Groups comprising the largest categories. This targeting pattern underscores a deliberate strategy to instill fear, deepen social divisions, and reinforce a militant in-group identity grounded in white supremacist and accelerationist ideologies.

Notably, the overlap in propaganda strategies between Terrorgram and other contemporary extremist movements, such as the Islamic State, highlights a convergence of digital tactics across ideological divides.

Furthermore, the integration of specific tactical guidance with emotionally charged and dehumanizing narratives lowers the threshold for violent action, particularly among lone actors. The frequent use of veiled and indirect threats, alongside direct calls for violence, amplifies the psychological impact of the material.

Future research should further explore the evolving architecture of far-right digital propaganda, with particular attention to its transnational dynamics and its capacity for narrative hybridization. Comparative analyses across different extremist milieus could shed further light on commonalities in communication strategy and consequently inform effective countermeasures.

Additionally, enhancing the detection and interpretation of threatening content on encrypted platforms remains a pressing challenge that necessitates interdisciplinary collaboration among researchers, policymakers, and technology providers. Addressing these gaps is essential for countering the operational effectiveness and psychological reach of entities like the Terrorgram Collective.

References

1. Barbarossa, E.: The three phases of terrorgram. Accelerationism Research Consortium (ARC) (2024), https://www.accresearch.org/accreports/the-three-phases-of-terrorgram, retrieved July 28, 2024
2. Basha, S.: 'death to the grid': Ideological narratives and online community dynamics in encouraging far-right extremist attacks on critical infrastructure. Counter Terrorist Trends and Analyses **15**(4), 17–24 (2023)

3. Byington, B.: Antisemitic conspiracy theories and violent extremism on the far right: A public health approach to counter-radicalization. Journal of Contemporary Antisemitism **2**(1), 1–18 (2019)
4. Hammer, H.L., Riegler, M.A., Ovrelid, L., Velldal, E.: THREAT: A Large Annotated Corpus for Detection of Violent Threats. 2019 International Conference on Content-Based Multimedia Indexing (CBMI) pp. 1-5 (Sep 2019)
5. Hammer, H.L.: Detecting threats of violence in online discussions using bigrams of important words. In: Proceedings of the 2014 IEEE Joint Intelligence and Security Informatics Conference. p. 319. JISIC '14, IEEE Computer Society, USA (2014)
6. Kingma, D.P., Ba, J.: Adam: A method for stochastic optimization (2017)
7. Kriner, M., Ihler, B.: Analysing terrorgram publications: A new digital zine. Global Network on Extremism and Technology (Sep 2022)
8. Li, J.: The pictorial turn and visual rhetoric: Analyzing image agency and persuasion in contemporary media. Advances in Humanities Research **9**, 31–35 (2024)
9. Lundmark, L., Kaati, L., Shrestha, A.: Visions of violence: Threatful communication in incel communities. In: 2024 IEEE International Conference on Big Data (BigData). pp. 2772–2778 (2024)
10. Macklin, G.: Praise the saints: The cumulative momentum of transnational extreme-right terrorism. In: A Transnational History of Right-Wing Terrorism, p. 26. Routledge, 1st edn. (2022)
11. Murib, Z.: Gender ideology, the far right, and lgbtq politics. PS: Political Science & Politics pp. 1–6 (2025)
12. O'Toole, M.E.: The School Shooter: A Threat Assessment Perspective. Federal Bureau of Investigation (Jan 1999)
13. O'Toole, M.E.: The school shooter: A threat assessment perspective. Tech. rep., Federal Bureau of Investigation, Critical Incident Response Group (CIRG), National Center for the Analysis of Violent Crime (NCAVC), FBI Academy, Quantico, Virginia (2000), supervisory Special Agent, PhD
14. Shrestha, A., Kaati, L., Akrami, N., Linden, K., Moshfegh, A.: Harmful communication: Detection of toxic language and threats on swedish. In: Proceedings of the 2023 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining. p. 624–630. ASONAM '23 (2024)
15. U.S. District Court, Eastern District of California: United states v. dallas erin humber and matthew robert allison. indictment (2024), case No. 2:24-cr-00257-DJC, U.S. District Court, Eastern District of California, 5 September 2024
16. Wester, A., Øvrelid, L., Velldal, E., Hammer, H.L.: Threat detection in online discussions. In: Proceedings of the 7th Workshop on Computational Approaches to Subjectivity, Sentiment and Social Media Analysis. pp. 66-71. Association for Computational Linguistics, San Diego, California (Jun 2016)
17. Winter, C.: The Virtual'Caliphate': Understanding Islamic State's Propaganda Strategy, vol. 25. Quilliam London (2015)
18. Zilvar, M.: "we are at war, white man! join the resistance and become the hero white people need": Analyzing collective action framing of the terrorgram collective's propaganda publications. Deviant Behavior pp. 1–17 (2025)