

Live-Streaming

Mapping Networks of Influence and (Dis)information Flow

Author(s)

van Boheemen, Pieter ; Bösch, Marcus; Costanzo, Giulia ; Divon, Tom; Frühwirth, Lea ; Hammelburg, Esther; Klüser, Jonathan ; Postma, Laura; Ring, Edan ; Steffen, Nina ; Wang, Xinlu

Publication date

2025

Document Version

Final published version

[Link to publication](#)

Citation for published version (APA):

van Boheemen, P., Bösch, M., Costanzo, G., Divon, T., Frühwirth, L., Hammelburg, E., Klüser, J., Postma, L., Ring, E., Steffen, N., & Wang, X. (2025). Live-Streaming: Mapping Networks of Influence and (Dis)information Flow. Web publication or website, .
<https://www.digitalmethods.net/Dmi/SummerSchool2025LiveStreaming>

General rights

It is not permitted to download or to forward/distribute the text or part of it without the consent of the author(s) and/or copyright holder(s), other than for strictly personal, individual use, unless the work is under an open content license (like Creative Commons).

Disclaimer/Complaints regulations

If you believe that digital publication of certain material infringes any of your rights or (privacy) interests, please let the Library know, stating your reasons. In case of a legitimate complaint, the Library will make the material inaccessible and/or remove it from the website. Please contact the library: <https://www.amsterdamuas.com/library/contact>, or send a letter to: University Library (Library of the University of Amsterdam and Amsterdam University of Applied Sciences), Secretariat, Singel 425, 1012 WP Amsterdam, The Netherlands. You will be contacted as soon as possible.

Live-Streaming: Mapping Networks of Influence and (Dis)information Flow

Team Members

Pieter van Boheemen - Post-X Society

Marcus Bösch - University of Münster

Giulia Costanzo - Politecnico di Milano

Tom Divon - The Hebrew University of Jerusalem

Lea Frühwirth - CeMAS(Center für Monitoring, Analyse und Strategie)

Esther Hammelburg - Amsterdam University of Applied Sciences

Jonathan Klüser - University of Zurich

Laura Postma - Netherlands Institute for Sound & Vision

Edan Ring (remote) - Ben Gurion University of the Negev and ISOC-IL

Nina Steffen - University of Zurich

Xinlu Wang - Tsinghua University

Key findings

This study explores how TikTok Live's fusion of immediacy, interactivity, and monetization creates a powerful infrastructure for political communication, one increasingly exploited for extremist mobilisation and disinformation. Focusing on far-right actors in Germany, it combines technical monitoring, content analysis, and policy review to examine how extremist networks exploit the platform's live-streaming affordances to spread propaganda, monetize hate, and evade moderation, often in ways that outpace both TikTok's self-regulation and external oversight under the EU's Digital Services Act (DSA).

Extremist networks thrive in TikTok Live's format. Far-right actors blend everyday conversation with extremist messaging, making Nazi propaganda feel socially embedded and more challenging to detect.

Coded language evades automated moderation. Dog whistles, symbolic references, and algospeak allow harmful narratives, including Holocaust praise and Hitler admiration, to circulate without triggering bans.

Monetization directly fuels harmful content. Virtual gifting not only sustains these Nazi networks but also provides TikTok with a revenue share (50%), effectively profiting from hate speech.

Parasocial intimacy amplifies influence. Live interactions, gifting, and features like TikTok's LIVE Match deepen audience loyalty, encouraging and mobilizing participation in extremist communities.

Platform enforcement prioritizes commercial risk. DSA-related moderation disproportionately targets TikTok Shop violations over violence, harassment, or privacy breaches, signaling a misalignment between stated safety priorities and actual practice.

Regulatory transparency is limited. Flaws in the DSA Transparency Database and TikTok's opaque documentation make it difficult for researchers and the public to assess how live content is governed.

Live-native moderation remains underdeveloped. Current safety measures focus on creator-managed moderation and post-hoc review, leaving a gap in real-time detection and intervention for harmful broadcasts.

Introduction

The Rise of Live-Streaming as a Political Medium

Live-streaming has emerged as a powerful real-time information-sharing medium across platforms like Twitch, YouTube Live, TikTok Live, Instagram Live, and Facebook Live. Unlike pre-recorded content, live streams convey an unfiltered immediacy that fosters authenticity and urgency. Combined with interactive tools like live chat, this real-time environment poses distinct challenges for moderation, fact-checking, and tracking the spread of disinformation.

The vulnerabilities exposed in live-streaming environments reflect a broader challenge across social media ecosystems, where the very conditions that make content engaging also make it vulnerable to manipulation. Disinformation proliferates six times faster than accurate information, thriving in spaces where speed, emotional engagement, and algorithmic amplification intersect; dynamics that extend well beyond live content (Surjatmodjo et al., 2024).

Within this landscape, TikTok has rapidly emerged as a pivotal force in political communication, fundamentally transforming the creation, dissemination, and consumption of political messages (Bösch & Divon, 2024; Uuamsky & Pipal, 2023). TikTok's distinct affordances, particularly its virality-driven algorithms and reduced dependence on follower counts, democratize content reach. However, these same features concurrently establish highly potent channels for the rapid amplification of content, including potentially misleading information.

The convergence of these dynamics presents a formidable challenge to information integrity and democratic discourse. Disinformation influencers deploy sophisticated, adaptive strategies that, when coupled with TikTok's rapid amplification systems and its tendency to blur the boundaries between entertainment and factual reporting, create fertile ground for the mass circulation of false narratives (Guinaudeau et al., 2022). Although TikTok provides political actors with unprecedented access to new audiences, it also necessitates a careful equilibrium between authentic interaction and the inherent risk of trivializing complex societal issues.

TikTok Live: Scale, Growth, and Governance Challenges

A striking illustration of this dynamic can be seen in the activities of right-wing extremists on German TikTok. An investigation by the journalism collective Firehose of Falsehood (2024) exposed how easily popularity can be engineered on a platform with 23 million German users (Morozova et al., 2024). Despite TikTok's claims about robust safety measures, analysts argue that the platform enables fabricated accounts to distort engagement metrics and boost content virality. The far-right AfD appears to have capitalized on these weaknesses, achieving exceptional reach in the months leading up to the 2024 European Election. Analyses show that AfD content consistently outperformed that of rival parties in both views and interactions.

A largely underexplored aspect of this landscape is live streaming on platforms like TikTok. TikTok Live has experienced rapid global growth, becoming the second most-watched streaming platform in Q1 2025, surpassing Twitch, primarily known for "In Real Life" (IRL) content (Streams Charts, 2025). The platform recently set a record with Tomorrowland's 2025 livestream, which drew over 74 million unique viewers and generated 2.4 billion video views during the two-week event (Goldstein, 2025). In that same quarter, TikTok Live recorded over eight billion watch hours across all live streams, representing a 30% increase from the previous quarter (Streams Charts, 2025). The live-streaming sector as a whole is experiencing significant growth, with projections estimating its value at 345.13 billion USD by 2030 and over one in four internet users engaging weekly with live streams (DemandSage, 2025). This growth illustrates the immense influence of live media and the urgency of examining how immediacy, interaction, and virality shape the circulation of information.

Beyond headline growth figures, TikTok's live-streaming ecosystem is defined by both its extraordinary scale and its governance challenges. The platform has approximately 1.5 billion active users (SearchLogistics, 2025), with an estimated 130 million going live each day (TikTok, 2025). In June 2025, simultaneous viewership peaked at 3.5 million accounts (TikTokStats, 2025). While TikTok applies moderation measures to live content, the European DSA Transparency Database contains thousands of entries referencing "LIVE" in TikTok's submitted Statements of Reasons (European Commission, July 3, 2025). However, the repository's flawed search function and the overall inaccessibility of these documents hinder meaningful scrutiny by researchers. This lack of transparency not only obscures how live-streaming issues are reported and addressed but also restricts the capacity of regulators and the public to oversee and respond to them effectively. We argue that these conditions underscore both TikTok Live's centrality to the platform and the broader difficulty of managing disinformation, harmful content, and platform manipulation in real time.

This project addresses growing concerns about the role of real-time media in participatory propaganda, the circulation of anti-democratic narratives, and the production of information disorder, particularly as live-streaming becomes increasingly accessible and mainstream. Focusing on TikTok as a primary site of analysis, our aim is to develop methodological approaches and tools for understanding how disinformation operates within live-streaming environments. We investigate the technical, social, and rhetorical affordances of the platform that enable the spread of false or misleading content. By mapping networks of influence, patterns of audience engagement, and practices of content repurposing, we seek to advance understanding of this emerging and highly influential mode of media consumption.

Research Questions

Main research question:

Which digital methods and tools can most effectively map, capture, and analyze the flow of disinformation narratives within TikTok Live?

Follow-up research questions that we probed into:

- 1) How do far-right networks leverage TikTok's live-streaming features to build connections and expand their audiences?
- 2) What types of coded language and symbols are used by far-right creators during TikTok Live streams to communicate extremist messages?
- 3) How does the ecology of exchange on TikTok Live, particularly gifting and interactive features, contribute to the spread of extremist content and potential monetization of hate

speech?

4) In what ways do TikTok's affordances for immediacy, authenticity, and ephemerality affect the dissemination of extremist propaganda and the perceived safety of live-streaming spaces?

5) How do TikTok's policies for moderating live streams align with, adapt to, or fall short of the external regulatory obligations imposed by frameworks like the EU's Digital Services Act?

Methodology

Initial Data Sets

By manually searching for tags (e.g., #afd), symbolic references (e.g., 'germanic'), and emojis (e.g., DE 🇩🇪) commonly associated with far-right communities, we compiled a dataset of 314 TikTok handles. Using a custom-built TikTok Live monitor tool, we recorded 107 fragments of live stream sessions and their accompanying metadata on the evening of July 2, 2025. This collection captured hundreds of minutes of streamed content, thousands of comments, account joins, gift transactions, new follower events, and stream shares.

Due to the ephemeral nature of live streaming, effective monitoring demands that researchers be present at precisely the right moment, adding both pressure and precariousness to the research process (Wa-Mbaleka, 2019). This challenge is compounded by the lack of no-code OSINT tools for investigating TikTok Live, as our search yielded none. To address this gap and enable the detection of digital threat communications on the platform, we explored multiple methodological approaches.

Data collection

Identifying accounts from pre-existing assets. A seed list of far-right TikTok accounts, compiled in earlier research via observation and algorithmic snowballing, served as the starting point. Additional leads were obtained by scanning prominent conspiracy and far-right channels on German Telegram for references to livestream activity, which revealed further accounts of interest.

Real-time identification based on content. Accounts were also identified in real time by searching TikTok Live for keywords, emojis, coded language, and "dog whistles" commonly used in far-right and pro-Russian circles. This approach yielded active accounts streaming at the moment of the search.

Automated monitoring of 314 accounts. Using a custom-built TikTok [Live monitor](#), we tracked 314 TikTok accounts on the evening of July 2, 2025, recording 107 fragments of live-stream sessions along with their metadata. This dataset included hundreds of minutes of footage, thousands of comments, records of accounts joining streams, gift exchanges, new follower activity, and stream shares. All videos were transcribed using a local implementation of OpenAI's Whisper.

Data analysis

We explored the dataset through a combination of manual and automated analysis: First, transcripts and comments were scored for toxicity using UnitaryAI's Detoxify tool (<https://github.com/unitaryai/detoxify>). Second, both transcripts and comments were analyzed for keyword occurrences with a custom Python script, drawing on a manually developed codebook (see attachments) containing terms related to conspiracy theories, xenophobia, hate speech, and extremist propaganda within the German context. Third, comments were examined for emoji frequency using another custom Python script. Fourth, gifts in each session were manually counted and converted into their corresponding monetary value. Fifth, a network analysis of users appearing in recorded comments and joins was conducted, with results visualized in Gephi. Sixth, recordings were manually screened (non-systematically) for potential propaganda, disinformation, or hate speech. Finally, in addition to the livestream dataset analysis, TikTok's policy on livestreaming was examined.

We note that keyword analysis of transcripts and comments, supported by a well-developed codebook, can help identify problematic language, but it is resource-intensive and demands contextual expertise. Automated searches are helpful in scanning large datasets, yet many harmful narratives are couched in everyday language, coded slang, or dog whistles that evade detection without human interpretation. While developing the codebook requires significant upfront effort, it enables more targeted, efficient review over time. In practice, effective moderation relies on combining automated data collection with informed human analysis.

*See [Code book german right-wing video transcripts - Blad1.pdf](#)

Findings

Narrative and Network Tactics

Incitements to violence and acts of doxing. In our dataset, we documented a case where a call to violence emerged following a [TikTok](#) Live "Match." Introduced in 2023, this feature enables two or four streamers to compete in real time, with the objective of securing the highest sum of micro-donations ("coins") from viewers. Competition is

often intensified by participants urging audiences to contribute aggressively. In one such session, this dynamic spilled over into the comments: viewers publicly disclosed the address of a streamer's corner shop, coupled with xenophobic insults targeting his non-German origins, and issued explicit incitements such as "storm the shop" and "pay him a visit."

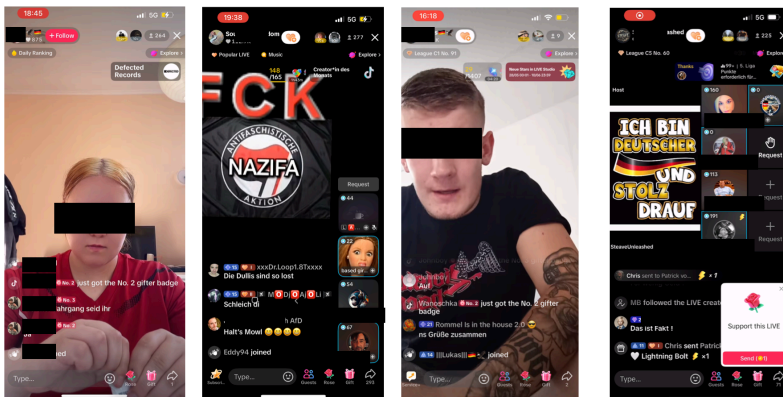


Image: Live Match featuring monetization prompts, nationalist slogans, antifascist counter-messaging, and xenophobic commentary

Seamless blending of casual conversation and propaganda. Many streams exhibited a fluid movement between mundane conversation and overt extremist messaging. Seemingly innocuous topics—such as the weather, breakfast routines, or reminders to apply sunscreen—were interwoven with personal anecdotes and, at times, explicit propaganda. In one case, a streamer repeatedly redirected casual exchanges toward discussions of participants' origins, using these as entry points into racial theorizing and didactic "history lessons" on the Third Reich. The affective register of these interactions often combined loneliness, humor, and gestures of social bonding, thereby naturalizing extremist narratives and embedding them within the rhythms of everyday exchange.

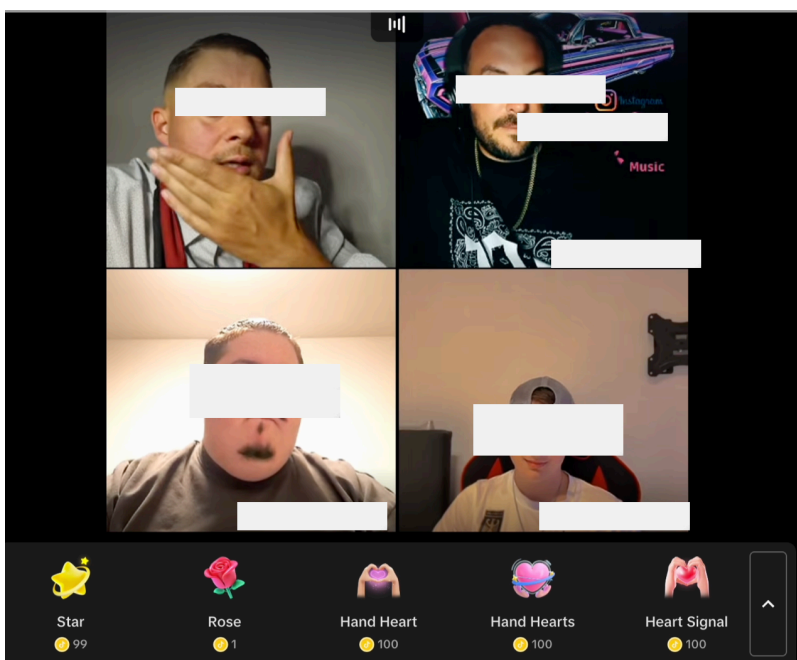


Image: TikTok Live where mundane conversation is interwoven with racial theorizing and extremist propaganda

Dog whistles and algospeak. Drawing on covert communication tactics such as dog whistles (Quaranto, 2022) and algospeak (Klug et al., 2023), streamers articulated Holocaust glorification and admiration for Hitler while deliberately avoiding keywords likely to trigger moderation. One recurring trope involved allegories about “baking six million cookies” with a “master baker and his servants”—a euphemism for the systematic extermination of approximately six million Jews by Nazi Germany between 1941 and 1945. These coded references were reinforced through contextual cues in the live chats: the repeated use of the letter “j” to signify Jews, and the sequential posting of “Sieg” and “Heil” across consecutive comments, which collectively erased any ambiguity about the intended allusions.

In some instances, third-party moderators were embedded within the streams to curb overt hate speech and reduce the risk of platform sanctions. Yet, even these interventions were saturated with extremist symbolism. In one case, a moderator adopted the username “Lagerarzt” (camp doctor) alongside a profile image of Nazi physician and war criminal Karl Gebhardt, infamous for coordinating medical atrocities at Ravensbrück and Auschwitz. Such acts underscore how moderation itself could be appropriated to reinforce, rather than disrupt, extremist meaning-making.

Gestures and Symbols. Our observations reveal how extremist streamers strategically mobilized clothing, symbols, and embodied gestures as coded signifiers of neo-Nazi affiliation. Apparel choices, for instance, functioned as semiotic cues: one streamer wore a Lonsdale T-shirt partially concealed by an unzipped hoodie so that only the letters “NS” remained visible, a shorthand for *Nationalsozialismus* (National Socialism). Similarly, material culture—such as various versions of the *Reichskriegsflagge* (Imperial War Flag)—was deployed as a proxy for the banned swastika flag. Profile images likewise circulated fascist visual codes: one user displayed a black eagle with outstretched wings, stylistically echoing the *Reichsadler* (Imperial Eagle). Although the swastika had been replaced with a football club crest, the original design language retained its resonance with Nazi iconography.

Gestural repertoires further reinforced these symbolic references. One streamer explicitly mimicked the theatrical poses Adolf Hitler practiced for his speeches in 1927, wrapping himself in a *Reichskriegsflagge* while performing these movements. Another example was more ambiguous but equally striking: a streamer executed the “dab”—a gesture popularized as a meme of triumph or playfulness—while dressed in a neo-Nazi outfit and accompanied by a Nazi pop song. Stripped from its original youth-culture context and reinserted into this extremist performance, the gesture visually approximated the Nazi

salute, demonstrating how memetic practices can be recontextualized to sustain fascist expression under the guise of popular culture.



We see an ecosystem in which propagandists, Nazi-affiliated rappers, AfD politicians, and TikTok creators operate in a mutually reinforcing circuit of influence, monetization, and ideological dissemination. We argue that this is less a loose constellation of actors than an infrastructural assemblage where cultural production, political messaging, and platform economies converge. Through monetization tools such as gifting and Live Matches, extremist narratives are commodified, turning ideology into content and content into capital. We see how TikTok's affective registers—its humor, intimacy, and virality—embed extremist discourse within ordinary patterns of entertainment and social exchange. In this configuration, the platform sustains extremist presence through algorithmic circulation while allowing hate to be disguised in casual conversation, memetic play, and aspirational self-branding. We argue that this produces a resilient formation that blurs the lines between politics and pop culture, propaganda and play, shifting extremist worldviews from the margins into normalized presence within the digital attention economy.

Recordings

Several fragments contain propaganda, disinformation, or hate speech.

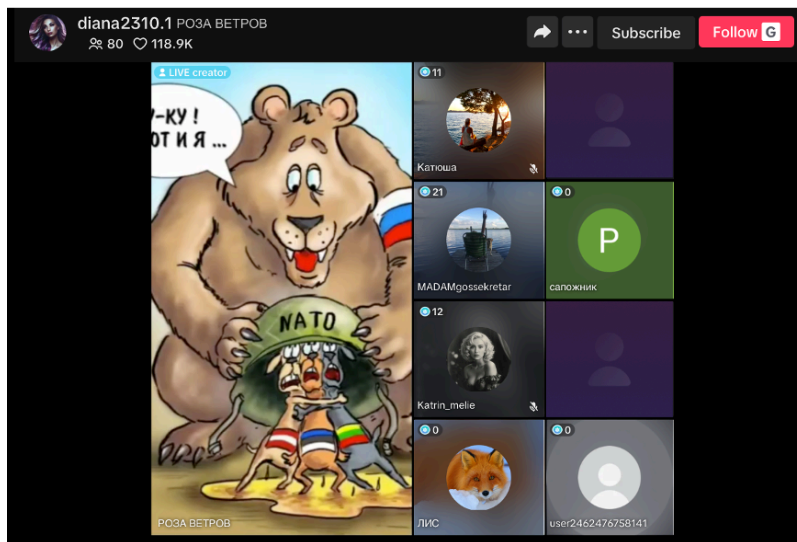


Image: Death threats in rap music

Noteworthy to mention the occurrences of algo-speak, e.g.: Commenters replace letters with numbers: “4usländer rau5 🤪 🤪 🤪 💙 💙” or “Diese linken und Grünen sind die N4zis” Or use symbolic references, such as “14”, “💜 💜 💜” or “88” Or emoji combinations, such as “😊😊”, “😊🧡” or “⚡ ⚡” There was also a lot of everyday chat, for example, about the weather.

Toxicity Levels in Comments

We analyzed 5,609 comments from livestream videos posted by German political TikTok users using Detoxify, an open-source model designed to detect toxic and offensive language. The model evaluates content across several categories: toxicity, severe toxicity, obscenity, threat, insult, identity attack, and sexual explicitness. All transcripts were analyzed, yielding 29 fragments with a toxicity score above 0.7. Of these, four were classified as obscene, one as threatening, five as insulting, and six as sexually explicit. Files:

<https://drive.google.com/drive/u/0/folders/1vMXp4HydkiQTJOZ7xEdstH7Gqe7sXGTA>

Minimal Explicit Hate Speech. Using a high-toxicity threshold of 0.7, only 26 comments —approximately 0.46% of the dataset—were flagged as highly toxic. The median toxicity score was just 0.0007, and the mean was 0.016, indicating that the vast majority of comments were either neutral or only mildly inappropriate. Although a handful of outliers approached the extreme end of the scale, they were statistically rare.

Obscenity and insults recorded the highest average scores (means ≈ 0.01 ; medians ≈ 0.003) and included the most extreme outliers (with maximums of 0.959 and 0.811, respectively). This points to occasional use of profanity or personal attacks, but not a sustained pattern of abuse. Other categories, such as severe toxicity, threats, identity attacks, and sexual explicitness, showed negligible presence (means below 0.002, medians under 0.001). Less than 0.18% of all comments were flagged as threatening or sexually explicit, and none exceeded 0.5 in identity attack. Notably, severe toxicity never surpassed 0.03.

Beyond Surface-Level Toxicity. While these findings may suggest that the comment sections of these political livestreams are largely benign, this absence of overt toxicity should not be misread as an absence of ideological harm. In the context of far-right propaganda, particularly livestreams aligned with neo-Nazi or extremist discourse, much of the harm operates through coded language, affective manipulation, and seduction-based propaganda that Detoxify’s technical parameters are not equipped to detect.

The low toxicity scores in this context may reflect not a healthier discursive environment, but rather a strategic sanitization of language to evade moderation while still pushing

harmful ideologies. This aligns with a broader shift in digital extremism: rather than spewing direct hate, many far-right creators now perform populism and irony, relying on aesthetic strategies and in-group cues that Detoxify does not classify as "toxic"—but which nonetheless amplify radicalization, normalize historical revisionism, and rehabilitate fascist symbols and narratives through algorithmically favored formats.

Implications. In short, toxicity detection models like Detoxify are limited in their ability to register the full scope of platformed political harm. Especially in environments shaped by far-right livestream aesthetics, harm is often discursively subtle, memetically wrapped, and designed to appear “non-toxic” while advancing racist, antisemitic, and anti-democratic logics. This calls for critical media scholarship that goes beyond automated detection to examine how platform affordances, moderation gaps, and livestream virality co-produce a hospitable terrain for algorithmically resilient fascist propaganda—not despite low toxicity, but precisely through it.

Emoji analysis

To bypass moderation, German right-wing extremists rely on algo-speak and coded dog-whistles, often embedding their messages in emoji use. Emojis function as both symbols and covert signals, appearing not only in comments during TikTok Lives but also in usernames to mark affiliation and circulate extremist concepts.

To systematically analyze this phenomenon, a custom Python script was developed to track emoji activity: recording frequency of use, the number of unique users deploying each emoji, and the most common emoji combinations. Each emoji was then manually coded into topical categories reflecting its semantic and political relevance—right-wing, left-wing, flags, religion, anti-Muslim, anti-LGBTQ, LGBTQ, conversational, or random.

The resulting visualization maps recurring emojis by positioning and sizing them according to both count and diversity of users. Their clustering highlights recurrent combinations, such as “❤️💜❤️” and “💀🔪,” which are recognizable extremist motifs. Finally, emojis were color-coded by topic to illustrate not only frequency but also the symbolic ecosystems through which extremist groups carve out communicative niches on TikTok.

Among the most frequently used emojis, several carry explicit significance within right-wing extremist discourse:

🇩🇪 German flag—invoked to signal nationalist identification.

💙 Blue heart—associated with pro-AfD sentiment, referencing the party’s signature color.

🦅 Eagle—read as Bundesadler (Germany's federal coat of arms) but also as Parteiadler, echoing the eagle iconography of the Third Reich.

♥️🖤❤️ Black-white-red—the colors of the German Imperial Flag (Reichsflagge, 1871–1945), often rendered as hearts, squares (🖤🖤🖤), or circles (🖤🖤🖤).

🙇 Saluting face—functioning as shorthand for the Nazi salute and “Heil Hitler.”

⚡️⚡️ Lightning bolts—referencing the insignia of the SS.

💀 / 🦴 Skull and crossbones—invoking the Totenkopf, emblem of the 3rd SS Panzer Division, an elite Waffen-SS unit.

🔪 Axe—evoking Viking-inspired imagery tied to survivalism and white-supremacist mythologies.

Gifting

The role of virtual gifting in TikTok's live-streaming economy. Virtual gifting is a primary revenue source for TikTok livestreamers, forming a central part of the platform's monetization system. TikTok currently offers around 230 different gift types, which viewers can buy and send to streamers. While digital, these gifts carry tangible monetary value, sustaining the economic viability of many livestreamers. Gifts are organized into tiers, and access to certain types is restricted to highly engaged platform members, creating a stratified participation model.

The logic of coins, membership, and monetization. To participate in gifting, viewers must first purchase TikTok coins (priced at roughly €0.01 per coin). TikTok uses promotional discounts to incentivize coin purchases and designs its gift tiers to encourage ongoing engagement. Certain high-tier gifts, especially “heart” gifts, are only available to active, high-engagement members. Gift ranks range from level 1 to level 50, determined by interaction frequency and intensity, effectively monetizing both intimacy and attention.

Gift visibility, availability, and ranking. Gift availability depends on the streamer's platform status and the timing of the broadcast. High-tier gifts, such as “Swim,” are generally reserved for high-ranking accounts and are rarely available in smaller streams. More common items—like “Autumn 2024,” “Rose,” and “Heart Me”—circulate widely. The gift menu is not arranged by price: mid-tier gifts often appear at the top, while expensive options such as “Galaxy,” “Gerry the Giraffe,” and “Swan” are buried further down. This design nudges users toward moderately priced gifts, reducing friction for repeat spending.

Observed gifting behavior and monetization of hate. From our empirical recordings, we identified 39 livestream clips in which gifting occurred. These ranged from a few minutes to several hours, with some viewers returning repeatedly. Notable streamers in our sample include: @b.i.w.a.k, @diana2310.1, @herr.graf.afd, @mkd.germanic, @nelsonpriess.afd, @pitstafffff, @ruskinemez, @sylviawi305, and @unbekannt2k24. Earnings ranged from tens to hundreds of euros per day, with the highest single-stream earnings reaching €114. Right-wing activists in these streams monetized their broadcasts through micro-donations while spreading hate speech. TikTok takes a significant percentage of each transaction — estimated at 50% of gift revenue — thereby directly profiting from this activity.

Read further to learn how TikTok's LIVE Gifts system operates, from rules and rewards to how audiences use them during livestreams -

https://docs.google.com/document/d/1f_hQEXql552LoF4NsSKv8KUUifRNgg6wZBlv1kV6224/edit?tab=t.0#heading=h.ta7buptty51e

TikTok Policy

TikTok's overarching stance on LIVE streaming is centered on fostering a positive and secure broadcasting environment, an approach articulated in three key policy documents: the LIVE Safety Guide, the Live Monetization Guidelines, and the Unlocking LIVE Monetization guide. Together, these documents set out TikTok's rules, recommendations, and prohibitions for creators on managing their livestreams. In the sections that follow, we unpack what TikTok identifies as its priorities for LIVE broadcasts and highlight critical blind spots in the platform's governance framework.

Before Going LIVE: Be safe and Real. TikTok has established a robust set of rules and resources to prepare creators before going live, framing them as tools to promote safe and responsible streaming. Yet, given that TikTok is now legally accountable for harmful activities on its platform (see the next section on the DSA), these measures should also be read as mechanisms for reducing the company's regulatory risk. First, creators are instructed to set visibility and tone by adjusting "content visibility" settings and using the "About Me" feature to communicate expectations, thereby "helping set the tone of the stream." Second, they are urged to know the rules, as outlined in the LIVE Safety Guide, which advises "familiarize yourself with our guidelines" to avoid unexpected disruptions or penalties. Age restrictions are explicit, with both creators and gift senders must be at least 18 years old, as stipulated in the LIVE Monetization Guidelines. Audience controls allow mature content to be restricted to adults, which TikTok frames as essential for "protecting viewers under 18." The LIVE Safety Guide also cautions against sharing exact locations or other sensitive information to protect personal privacy. Finally, authenticity is positioned as a core principle, with creators reminded that "LIVE is a space for being yourself" and that impersonation is strictly prohibited.

During LIVE: Management and Control Features. Once a LIVE broadcast begins, TikTok provides creators with tools to maintain a platform-safe environment, combining engagement features with moderation controls. The first category includes safety and interactive options from the LIVE Safety Guide, such as LIVE Match, which enables head-to-head competitions with other streamers while allowing hosts to control Multi-Guest, which supports collaborative or panel-style streams but requires active oversight of guest behavior. The second is the LIVE Safety Education Center, offering tutorials and best practices on managing disruptions, identifying harmful behavior, and setting clear audience rules—skills essential for minimizing real-time risks. To further manage community interactions, creators can disable comments, apply keyword filters to block offensive terms, or mute disruptive viewers either temporarily or permanently. Framed by TikTok as tools for “controlling your chat,” these functions help streamers shape the tone of their broadcasts and protect audiences from abuse. The platform repeatedly emphasizes that creators should “actively moderate their streams,” reflecting a user-centered liability model in which hosts bear primary responsibility for live moderation, supported by a Safety Team that monitors streams in real time and intervenes when community standards are violated, aligning broadcasts with platform policy and evolving regulatory expectations.

LIVE Money: Monetization and Sales Policies. Monetization is central to TikTok LIVE, but it operates within clear parameters set out in the LIVE Monetisation Guidelines and the Unlocking LIVE Monetisation guide. These resources outline how creators can earn through micro-donations known as LIVE Gifts, which viewers purchase to “show support during your LIVE.” Eligible creators may receive up to 50% of TikTok’s net revenue from these gifts, a revenue-sharing model designed to incentivize engagement. Gamified features such as Lucky Airdrop Boxes and LIVE Battles further enhance monetization opportunities, blending entertainment with audience participation. At the same time, the guidelines explicitly prohibit the sale of illegal or regulated goods and underscore TikTok’s emphasis on authenticity, reminding creators to “Be Yourself,” even when monetizing.

LIVE as a “Hotbed for Bad Actors”: Blindspots. While TikTok’s official documentation outlines proactive measures for managing LIVE content, it also exposes substantial vulnerabilities. First, the LIVE Safety Guide acknowledges that the ephemeral nature of broadcasting enables harmful content to circulate rapidly before moderation can intervene. Second, while age restrictions are specified, no robust verification mechanisms are detailed, allowing malicious actors to bypass safeguards. Third, the policy fails to address how the recommendation system may algorithmically amplify extremist content that gains early engagement, enabling it to spread widely. Fourth, monetization features such as LIVE Battles and Lucky Airdrop Boxes, promoted in the Unlocking LIVE Monetization guide, risk incentivizing provocative or sensational behavior to attract gifts and rewards. Finally, despite repeated emphasis on “authenticity,” the

guidelines lack clear strategies for detecting or preventing sophisticated impersonation tactics, including deepfakes, which could be used to pose as credible individuals or victims to disseminate misinformation.

TikTok LIVE Enforcement Under the DSA: A Glimpse

Platform-level commitments are increasingly required to align with binding obligations set by regulatory bodies, most notably the DSA. Unlike TikTok's self-imposed guidelines, the DSA establishes enforceable legal duties for Very Large Online Platforms (VLOPs) such as TikTok, directly shaping their governance of content, including live streams. Its most stringent provisions are designed to close gaps in self-regulation, ensuring that systemic risks linked to live broadcasts are identified, assessed, and addressed with legal accountability.

Specifically, Article 16 requires platforms to implement robust notice-and-action mechanisms enabling users to report illegal content, ensuring timely responses to harmful material, including that disseminated during live streams (Art. 16). Article 34 obliges platforms to "identify, analyze and assess any significant systemic risks," highlighting the "dissemination of illegal content through their services"—a risk particularly acute for real-time, ephemeral formats such as live broadcasts (Art. 34). Building on this, Article 35 mandates "reasonable, proportionate and effective mitigation measures," which involve adjusting recommendation algorithms and strengthening moderation systems to curb the rapid spread of illegal or harmful live content (Art. 35). Article 37 further imposes transparency, requiring the publication of content moderation reports, including user notices and removal actions, thereby enhancing public accountability (Art. 37). Finally, Article 22 establishes the role of accredited trusted flaggers, whose reports must be prioritized, integrating external oversight into moderation workflows and reinforcing protections for users exposed to harmful live broadcasts (Art. 22). Collectively, these provisions replace voluntary platform policies with a comprehensive, legally binding framework that compels platforms to systematically address the unique risks of areas like live streaming, safeguard user rights, and maintain transparency in handling harmful or illegal content.

To examine how these regulatory expectations play out in practice, we analyzed a dataset of 778 livestream-related moderation decisions from TikTok, sampled on July 2, 2025. While this represents only a single day's enforcement snapshot, it offers a valuable cross-section of the platform's approach to livestream moderation under the DSA's transparency and accountability requirements. The vast majority of takedowns (713 cases) stemmed from violations of TikTok Shop terms—most notably "engaging in activities that breach our TikTok Shop Creator Terms of Use" (666 cases) or "publishing low-quality content and/or exhibiting abnormal uploading frequency" (33 cases). Violent content accounted for 38 removals, flagged for "Violent Behaviors" or "shocking and

graphic content.” Another 18 removals involved data protection and privacy breaches, such as exposing “Personal Information – High Risk.” More minor but notable categories included five cases of intellectual property infringement, unauthorized trademark use, and four cases of real-time scams. Nearly all takedowns were initially flagged by automated systems. Still, final decisions were confirmed manually (“AUTOMATED_DECISION_NOT_AUTOMATED”), underscoring TikTok’s hybrid enforcement model, combining algorithmic detection with human oversight.

Discussion

TikTok deploys multiple moderation tools—including content monitoring, fact-checking, and removal—to address harmful or misleading material (TikTok, 2025). Interventions such as fact-checking, content labeling, and community notes have been shown to flag and correct misleading narratives in other social media contexts (Hameleers & Tulin, 2022). Yet, our findings point to shortcomings in applying these mechanisms to live streaming. The real-time nature of broadcasts makes it challenging to monitor streams as they happen, verify spoken content on the spot, or issue timely corrections. In our case study of far-right actors in Germany, we observed consistent use of non-explicit “algo-speak,” and coded references designed to slip past automated hate speech detection. These tactics blunt the effectiveness of conventional disinformation countermeasures, raising doubts about whether tools proven in other contexts—e.g., fact-checking—are meaningfully deployed in live-stream environments. Addressing these gaps will require moderation strategies explicitly tailored to the dynamics of live streaming rather than relying on frameworks built for static or recorded content.

Our data also reveals a striking enforcement imbalance. While TikTok’s actions meet the DSA compliance, they disproportionately target commercial violations—particularly breaches of TikTok Shop terms—with greater consistency than serious harms such as violence, privacy violations, or scams. This prioritization suggests that the platform acts most decisively when its own commercial ecosystem is at stake, treating user safety and the mitigation of offline harms as secondary concerns. By allowing high-impact, harmful content to remain visible until after manual review, TikTok’s current approach risks undermining both the spirit of the DSA and its own stated safety commitments. This pattern reflects not just operational challenges, but a misalignment between regulatory compliance as performed on paper and the substantive protection of users in practice.

Conclusions

Live Streaming as Propaganda Infrastructure

This study shows that TikTok Live is not simply an entertainment feature but a high-speed, high-reach communications infrastructure where immediacy, interactivity, and

affect are core drivers of influence. Within this environment, far-right networks in Germany have adapted platform affordances—from competitive formats like LIVE Match to monetization tools like gifting—to cultivate loyal audiences, translate attention into revenue, and seed extremist narratives. These narratives are not always delivered through overt calls to action; instead, they often slip between moments of everyday chat, humour, and personal sharing, which makes them both more socially acceptable and more resistant to detection. The blending of the banal with the extreme, coupled with coded language and visual cues designed to evade automated moderation, reveals a propaganda style that thrives in the intimate, parasocial dynamics of live streaming.

Our findings also surface a structural tension in TikTok's governance of live content. While the platform invests in moderation tools and policy frameworks, its enforcement patterns under the DSA appear disproportionately focused on protecting its commercial ecosystem, particularly TikTok Shop, rather than addressing serious harms such as violence, harassment, or privacy violations. This imbalance suggests that safety is treated less as a foundational principle and more as a regulatory compliance requirement to be met selectively. The reliance on post-hoc manual confirmation means that harmful live content can circulate during its peak moment of influence, effectively eroding the real-time protective capacity that live environments demand. In practice, TikTok's current approach manages reputational and regulatory risk for the platform more effectively than it mitigates societal risk for its users.

Implications and Future Directions

The implications are wide-reaching. Societally, the monetization of harmful live content risks entrenching extremist networks, normalizing dangerous rhetoric, and directly funding its spread. This calls for stronger mechanisms to ensure that the same urgency applied to commercial violations is applied to protecting public safety, particularly where live content has offline consequences. Academically, this research underscores the need for methodological innovation in capturing, preserving, and analysing ephemeral content, as well as for theories that account for the hybrid space where entertainment logics, platform governance, and extremist mobilisation intersect. Technically, there is an urgent need for moderation systems designed specifically for live streaming—including real-time detection of coded speech, proactive escalation protocols for high-risk streams, and integrated transparency tools that allow regulators and researchers to audit live enforcement in meaningful ways.

Future research should broaden this analysis beyond a single national case to map how extremist actors operate across languages, cultures, and platforms, and how their tactics adapt to different governance regimes. This should be paired with technical pilots that test the feasibility of live-native moderation interventions, as well as policy research into how regulations like the DSA can be operationalised for the unique challenges of live

media. Addressing these issues will require collaboration between researchers, civil society, regulators, and platform engineers. Without such cross-sector engagement, the gap between regulatory intent and actual protective outcomes will remain, and live streaming will continue to be both one of the most participatory and most exploitable spaces in the digital ecosystem.

Recommendations

Based on our findings, addressing the risks of harmful livestream content on TikTok requires interventions that are proactive, live-specific, and balanced in their enforcement priorities. Central to this is enhancing the ability to detect problematic accounts before or during harmful broadcasts. Extensive observation and snowballing should be core elements of monitoring workflows, enabling researchers, regulators, and civil society actors to surface networks of connected accounts.

Practical detection angles can be integrated into this process: Checking the Live button in a user's bio to access previous or scheduled streams. Searching for usernames within TikTok's live section for hints of live activity. Reviewing a user's regular TikToks for references to past or upcoming streams. Cross-checking other platform profiles (e.g., YouTube Live tabs) to confirm livestreaming as part of their content repertoire. Using TikTok's standardized live URL format (www.TikTok.com/@handle/live) with the Wayback Machine to uncover archived live activity, where available.

Societal. Civil society organisations and watchdog groups should incorporate these detection strategies into real-time monitoring, enabling earlier flagging of high-risk accounts and supporting timely countermeasures. Public literacy campaigns can raise awareness of how monetization incentives drive harmful behaviour during live streams.

Academic. Researchers should refine and test detection protocols across multiple cultural and linguistic contexts, developing replicable toolkits for identifying, capturing, and archiving ephemeral live content. Collaborative projects between computational and qualitative researchers can improve both coverage and contextual interpretation.

Technical. Platforms should operationalise detection angles within internal moderation systems, integrating them with live-native tools capable of identifying coded language, symbolic references, and behavioural cues in real time. Automated triggers for high-risk streams should prompt rapid human review and, where necessary, immediate intervention before peak audience engagement.

Policy. Regulators should ensure that enforcement under frameworks such as the DSA does not over-prioritise commercial violations at the expense of user safety. Live-specific risk assessment and mitigation requirements—such as those outlined in Articles 16, 34,

and 35—should explicitly address the detection and interruption of harmful streams in real time.

Bibliography

Bösch, M., & Divon, T. (2024). The sound of disinformation: TikTok, computational propaganda, and the invasion of Ukraine. *new media & society*, 26(9), 5081-5106.

Cervi, L., & Divon, T. (2023). Playful activism: Memetic performances of Palestinian resistance in TikTok# Challenges. *Social Media + Society*, 9(1), 20563051231157607. <https://doi.org/10.1177/20563051231157607>

nowiki>DemandSage. (2025, May 21). 42 live streaming statistics 2025: Trends and growth. Retrieved from <https://www.demandsage.com/live-streaming-statistics/>

European Commission. (2025). Transparency reporting: TikTok – statements of reasons referencing “LIVE” [Dataset]. Digital Services Act Transparency Database. Retrieved from https://transparency.dsa.ec.europa.eu/statement?s=LIVE&platform_id%5B%5D=30&platform_id-30=on&created_at_start=&created_at_end=

Goldstein, H. (2025, August 8). Tomorrowland shatters TikTok livestream record with 74 million viewers. EDM. <https://edm.com/news/tomorrowland-2025-breaks-record-biggest-live-event-TikTok-live-history/>

Hameleers, M., & Tulin, M. (2022, December 7). White paper: Making fact-checks work – Evidence-based recommendations for practitioners (BENEDMO D16). BENEDMO. Retrieved July 4, 2025, from https://benedmo.eu/wp-content/uploads/2022/12/D16_-_Recommendations-on-effectiveness-of-fact-checkers_website-version.pdf

Klug, D., Steen, E., & Yurechko, K. (2023, April). How algorithm awareness impacts algospeak use on TikTok. In *Companion Proceedings of the ACM Web Conference 2023* (pp. 234-237).

Morozova, A., Stănoiu, I., Stefankova, E., Šlerka, J., Malts, K., Blum, P., & Zubor, Z. (2024, July 3). How the far-right used TikTok to spread lies and conspiracies. VSquare. Retrieved from <https://vsquare.org/far-right-TikTok-lies-conspiracies/>

Quaranto, A. (2022). Dog whistles, covertly coded speech, and the practices that enable them. *Synthese*, 200(4), 330.

nowiki>SearchLogistics . (2025, April 1). TikTok user statistics 2025: Everything you need to know. Retrieved from <https://www.searchlogistics.com/learn/statistics/TikTok-user-statistics/>

Streams Charts. (2025). Q1 2025 global livestreaming—TikTok Live surpasses Twitch. [StreamsCharts.com](https://streamscharts.com/news/q1-2025-global-livestreaming). Retrieved from <https://streamscharts.com/news/q1-2025-global-livestreaming>

Surjatmodjo, D., Unde, A. A., Cangara, H., & Sonni, A. F. (2024). Information pandemic: A critical review of disinformation spread on social media and its implications for state resilience. *Social Sciences*, 13(8), 418. <https://doi.org/10.3390/socsci13080418>

TikTok. (n.d.). Combating misinformation. TikTok Transparency Center. Retrieved July 4, 2025, from <https://www.TikTok.com/transparency/en-us/combating-misinformation/>

TikTok. (2025, June 23). Celebrating community and creativity: TikTok LIVE kicks off Community Fest 2025. TikTok Newsroom. Retrieved from <https://newsroom.TikTok.com/en-us/community-fest-2025>

Umansky, N., & Pipal, C. (2023). Dances, duets, and debates: Analysing political communication and viewer engagement on TikTok. OSF Preprints. <https://doi.org/10.31219/osf.io/preprints/psyarxiv/>

Wa-Mbaleka, S. (2019, September). The researcher as an instrument. In *World Conference on Qualitative Research* (pp. 33–41). Cham: Springer International Publishing. https://doi.org/10.1007/978-3-030-15200-0_4

Sources used to develop the code book

Carnegie Endowment for International Peace. (2025, June). The new global struggle over gender rights and family values. <https://carnegieendowment.org/research/2025/06/the-new-global-struggle-over-gender-rights-and-family-values?lang=en>

Citizens for Ethics. (n.d.). Trump has spread conspiracy theories about January 6th more than 175 times on Truth Social. Retrieved July 4, 2025, from <https://www.citizensforethics.org/reports-investigations/crew-investigations/trump-has-spread-conspiracy-theories-about-january-6th-more-than-175-times-on-truth-social/>

Correctiv. (2025, February 20). 14 Beispiele für völkisches Denken in der [AfD](https://www.afd.de/). <https://correctiv.org/aktuelles/neue-rechte/2025/02/20/14-beispiele-fuer-voelkisches-denken-in-der-afd/>

EBSCO. (n.d.). Great replacement theory (white replacement theory). Retrieved July 4, 2025, from <https://www.ebsco.com/research-starters/political-science/great-replacement-theory-white-replacement-theory>

European Commission. (2021). Conspiracy theories and right-wing extremism: Insights and recommendations for P/CVE. Radicalisation Awareness Network (RAN).

https://home-affairs.ec.europa.eu/networks/radicalisation-awareness-network-ran/publications/conspiracy-theories-and-right-wing-extremism-insights-and-recommendations-pcve-2021_en

European Parliament. (2021). Disinformation about LGBTI+ persons and rights. Think Tank. [https://www.europarl.europa.eu/thinktank/en/document/EXPO_BRI\(2021\)653644](https://www.europarl.europa.eu/thinktank/en/document/EXPO_BRI(2021)653644)

Konrad-Adenauer-Stiftung. (n.d.). *Rechtsextreme Codes*.

<https://www.kas.de/de/web/extremismus/rechtsextremismus/rechtsextreme-codes>

Nordskov Media, & Flickr. (n.d.). (Image). (2025). In Youth, TikTok and the far right: A growing concern across Europe. Organized Crime and Corruption Reporting Project (OCCRP). [https://www.occrp.org/en/news/youth-TikTok-and-the-far-right-a-growing-concern-across-europe#:~:text=Far%2Dright%20extremists%20now%20use,Nordskov%20Media%2C%20Flickr%2C%20License\)](https://www.occrp.org/en/news/youth-TikTok-and-the-far-right-a-growing-concern-across-europe#:~:text=Far%2Dright%20extremists%20now%20use,Nordskov%20Media%2C%20Flickr%2C%20License))

Organized Crime and Corruption Reporting Project (OCCRP). (n.d.). Youth, TikTok and the far right: A growing concern across Europe. Retrieved July 4, 2025, from [https://www.occrp.org/en/news/youth-TikTok-and-the-far-right-a-growing-concern-across-europe#:~:text=Far%2Dright%20extremists%20now%20use,Nordskov%20Media%2C%20Flickr%2C%20License\)](https://www.occrp.org/en/news/youth-TikTok-and-the-far-right-a-growing-concern-across-europe#:~:text=Far%2Dright%20extremists%20now%20use,Nordskov%20Media%2C%20Flickr%2C%20License)

Pennycook, G., & Rand, D. G. (2020). White consciousness helps explain conspiracy thinking. Harvard Kennedy School Misinformation Review.

<https://misinforeview.hks.harvard.edu/article/white-consciousness-helps-explain-conspiracy-thinking/>

PMC. (2020). PMID: 32412117. (PMC7251254).

<https://pmc.ncbi.nlm.nih.gov/articles/PMC7251254/>

United States Holocaust Memorial Museum. (n.d.). Protocols of the Elders of Zion. Retrieved July 4, 2025, from

<https://encyclopedia.ushmm.org/content/en/article/protocols-of-the-elders-of-zion#:~:text=The%20purpose%20of%20these%20contemporary,antisemitic%20conspiracy%20theories%20about%20Jews>.

UN Women. (2024, May). LGBTIQ communities and the anti-rights pushback: 5 things to know. <https://www.unwomen.org/en/news-stories/explainer/2024/05/lgbtiq-communities-and-the-anti-rights-pushback-5-things-to-know>

VSquare. (n.d.). Far-right TikTok lies, conspiracies. Retrieved July 4, 2025, from <https://vsquare.org/far-right-TikTok-lies-conspiracies/>

 Attachments 9

This topic: Dmi > SummerSchool2015 >

SummerSchool2015ProjectsWeek1 > SummerSchool2025LiveStreaming

Topic revision: