

FROM SOCIAL NOISE TO ENTERPRISE RISK: ALIGNING COMMS, LEGAL, AND SECURITY IN THE ERA OF HARD TO MONITOR SOCIAL PLATFORMS

AN EDELMAN ANALYSIS IN PARTNERSHIP WITH OSAVUL

An analysis of reputational threats on hard-to-monitor platforms (such as TikTok and Telegram) shows how these are now tightly tied to legal, operational and physical risk, potentially creating real liability, safety, and operational disruption, and in some cases acting as potential precursors to cyber or real-world harm on top of 'typical' reputational risk. Many organisations may be blind to these threats until it's too late.

The analysis reveals a corporate threat surface that is broader, faster moving, and more closely linked to enterprise risk than most organisations are currently structured to manage. The solution is organizational: integrate communications, legal, intelligence and security around shared detection, playbooks, and measurable escalation thresholds.

This is a warning about adversarial storytelling that exploits moments of reputational vulnerability, regulatory exposure, social tension, and operational disruption to shape perception faster than organisations can identify the threat, validate facts, align internally, and respond with credibility.

The data points to a shift in kind, not just in volume. Reputational threats are aligning with enterprise risk in ways that challenge existing governance, escalation, and ownership models.



Dmytro Bilash
CBDO &
Co-founder, Osavul
d.bilash@osavul.cloud



Oliver Hayes OBE
EMEA Head of Counter-Disinformation, Edelman
oliver.hayes@edelman.com



Dave Fleet
Global Head of Digital Crisis, Edelman
dave.fleet@edelman.com

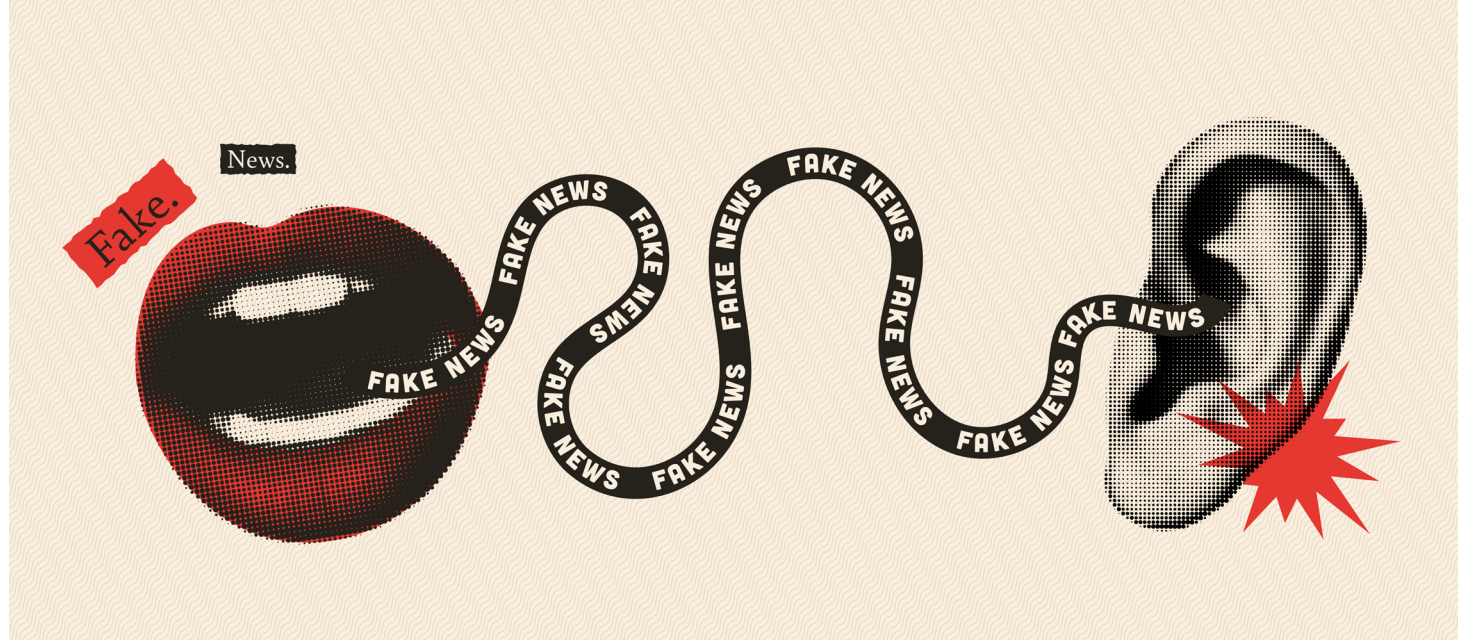
WHAT THE DATA SHOWS — AND WHY IT MATTERS

The underlying data collection and threat intelligence analysis were conducted by Osavul, an AI company specializing in strategic intelligence and countering hybrid threats. Osavul leveraged its AI platform, Nebula, to carry out a three-step analytical process:

- Collection of precise data from hard-to-monitor networks using Osavul's proprietary data pipeline technology.
- Extraction of stable and evolving narratives from the dataset through Osavul's AI-powered narrative intelligence technology.
- Identification of threats within narratives exhibiting indicators of malicious activity, using Osavul's threat intelligence capabilities.

Osavul's threat-intelligence dataset, reviewed by Edelman's Counter-Disinformation Unit, covers six months of TikTok and Telegram content relating to 130 global brands and sectors between 1st June and 1st December, 2025. Of those, 76 were the subjects of adverse reputational narratives. In total, 1,271 distinct narratives were detected, which comprised at least 25,053 messages and generated approximately 3.37 billion views where reach data was available.

Osavul categorised each threat across multiple dimensions: target type (company, product or service, leadership, industry); threat type (legal or regulatory, physical, technical, reputational, among others); subtype themes; platform dynamics; language; and geographic indicators. Some individual threats spanned multiple categories, but the dominant patterns were consistent.



LEGAL AND PHYSICAL NARRATIVES DOMINATE THE THREAT LANDSCAPE

Almost three-quarters of adverse narratives (71 percent) suggested some form of legal or compliance problem for the target organisation, making this the single most prevalent threat category.

More than half (56 per cent) suggested physical world risks such as civil unrest or criminal activity. These narratives were anchored in storylines that sound plausible, are difficult to rebut quickly, and can trigger real stakeholder consequences, including investigations, litigation, protests, criminal activity, and safety incidents.

Across the dataset, allegations of compliance violations appeared 532 times, political or civil unrest 501 times, regulatory investigations 404 times, criminal activity 361 times, and lawsuits 306 times.

This pattern challenges a common organisational assumption: that defending against adverse narratives is solely about countering clear fabrications and therefore easily disproved.

Today's threat environment is a grey zone. Selectively true claims, exaggerated allegations, clips taken out of context, and coordinated amplification of unresolved issues keep organisations on the defensive without relying on a single provably false statement.

Implication for leaders: An approach centred on fact-checking alone is insufficient and not aligned with the threat, leaving organisations exposed when scrutiny is highest.

Instead, organisations need a holistic approach to insulating their key stakeholders from misleading interpretations and contesting the narrative space.

RISK EXPOSURE REFLECTS SECTOR SENSITIVITY AND COMPANY PROMINENCE

Threat activity is not evenly distributed across the corporate landscape. It tends to concentrate around organisations that combine high public visibility with exposure to politically or socially sensitive issues.

In the dataset, the five most-targeted brands account for more than half (59 per cent) of detected threats. These organisations are typically large, well-known companies operating in sectors that attract regulatory scrutiny, geopolitical attention or public controversy. Global technology platforms, infrastructure providers, and companies operating in strategically sensitive industries feature prominently.

This concentration reflects how adversarial actors allocate attention and resources. They focus where narratives are most likely to resonate with existing public debate, spread quickly across platforms and exert pressure on companies through stakeholders, regulators or political actors.

Implication for leaders: Risk exposure is shaped not only by company prominence but also by sector dynamics and the sensitivity of particular issues.

Organisations operating in contested or highly regulated sectors may face heightened narrative risk regardless of their scale. Leaders should assess their exposure accordingly and ensure their preparation reflects the realities of their sector as well as their visibility.

ADVERSARIAL NARRATIVES OFTEN CENTRE ON PRODUCTS AND OPERATIONS

The dataset reveals that adversarial narratives focus on operational issues more than many communications teams might expect. These narratives focus on the institution of the company in 1,196 instances, associated with 23,619 messages and approximately 3.33 billion views.

Adversarial narratives focus on products and services across 876 instances, linked to 17,342 messages and approximately 2.03 billion views (with some narratives spanning both categories).

Adversarial narratives can attach themselves to what people buy, use, or rely on day to day. Themes such as compliance, safety, and criminality map directly onto stakeholder decision-making. Is this safe? Is it ethical? Is it legal? Is it trustworthy?

Operationally-based narratives travel so effectively because they make abstract reputational themes feel tangible. They align with real-world anxieties and force organisations into responding to complex issues across functional boundaries.

Implication for leaders: Adverse narratives now act as a product and operational risk multiplier, amplifying scrutiny and accelerating decision pressure across the organisation.

LEADERSHIP TARGETING IS LOWER IN VOLUME BUT HIGHER IN IMPACT

Narratives focused on leadership and executives appear less frequently than narratives focused on companies or products, but when they do occur their impact is significant. The dataset includes 142 narratives targeting leaders, generating 3,040 messages and approximately 787 million views. These topics gain traction.

Leadership narratives compress complex organisational issues into simple storylines that are easier to personalise, weaponise, and mobilise around. They travel efficiently in short-form video formats and can escalate quickly into harassment, intimidation, and physical security risks.

Implication for leaders: Personal risk monitoring and protective intelligence should be treated as essential capabilities, not as discretionary or reactive measures.

THE ECOSYSTEM IS MULTILINGUAL AND CROSS-BORDER BY DEFAULT

Threat amplification occurs across multiple languages, led by English, Italian, and Russian, followed by German, Spanish, Portuguese, Ukrainian, Romanian, and French. Narratives can move across platforms, borders and languages before appearing in mainstream channels, while it is hard to identify, attribute, and track specific threat actors.

Implication for leaders: Monitoring limited to English-language content or mainstream platforms may miss early warning signals, upstream narrative formation, and coordination activity.

KEY STATISTICS AT A GLANCE

- **130** brands analysed; **76** showed identifiable threats
- **1,271** hostile narrative threats detected across six months
- **25,053** messages linked to those threats
- Approximately **3.37 billion** views recorded where reach data was available
- Approximately **71.5 per cent** of threats carried legal or regulatory signals
- Approximately **56.1 per cent** carried physical-world risk signals
- Threat concentration: top five brands account for approximately **59 per cent** of threats



Listen to our recent discussion
to learn more about the growing impact of these adversarial narratives on major global corporations.

WHAT SENIOR LEADERS SHOULD DO NOW

If reputational threats are converging with enterprise risk, then organisations' response must mirror this. Fragmented ownership slows response and compounds the problem. There are several steps that leaders can take now to address this:

Create a cross-functional narrative response cell

High-performing organisations align communications, intelligence, legal, and security teams around a shared view of the threat landscape.

Map narrative exposure like a risk register

Recurring themes such as compliance, investigations, unrest, criminality, and cyber activity should be treated as predictable attack vectors.

Organisations can often 'pre-bunk' these narrative attacks by communicating counter-arguments to their key audiences in advance.

Develop and test platform-appropriate playbooks and content

The reach and impact of hard-to-monitor platforms demand rapid, credible, and appropriate responses.

Organisations should not wait for a reputational attack to escalate and spread before trialling their playbook; they should simulate adverse narratives appearing on hard-to-monitor platforms and spreading to mainstream channels to stress test their plans.

Organisations should also develop rapidly deployable digital assets for dissemination at pace in the event of a narrative attack.

Invest in advanced monitoring and detection capabilities

Many companies' standard social media monitoring cannot effectively track content on TikTok, Telegram or similar platforms.

You need to see it to analyse it. Adversarial content can go viral quickly, and organisations need to know what they can safely ignore versus where they need to intervene early.

Establish rapid decision-making procedures

Narrative attacks move quickly, but organisational decision-making often does not.

Companies should predefine escalation triggers, decision authority and response ownership across communications, legal and security teams. When these pathways are clear in advance, organisations can respond faster and with greater confidence.

THE BOTTOM LINE

The appearance of adverse narratives on hard-to-monitor platforms is not a niche concern. It acts as an accelerant, attaching itself to issues around legal exposure, operational disruption, physical safety, cyber vulnerability, and stakeholder trust.

Organisations that continue to treat this as a separate social media problem will remain in a reactive crouch.

Those that recognise it as an integrated enterprise threat, and respond with early detection, cross-functional authority, and disciplined decision-making, will be better positioned to protect trust, reduce harm, and sustain resilience in an increasingly volatile information environment.