A Longitudinal Analysis of Temporal Anomaly Detection in Telegram Cybersecurity Channels

dr. Andrius Daranda, dr. Lina Kankevičienė, Julija Daranda

Alytus Faculty, Kauno kolegija Higher Education Institution

ABSTRACT

The dramatically increasing volume of information on social media significantly enhances real-time assessment of cybersecurity threats. In this research, 9,415 messages from 9 public Telegram channels were analyzed over 360 days. A multi-method statistical framework was implemented to detect significant deviations in activity through triangulated metrics: Z-score analysis, percentage change detection, and composite scoring.

The analysis identified 101 anomalous days (28.1% of the observation period), with 80% of the top-10 spikes successfully attributed to real-world incidents, including data breaches, zero-day vulnerabilities, and geopolitical cyber operations. Clear temporal patterns emerged: activity concentrated on weekdays, with January accounting for approximately one-third of all yearly anomalies and 62.1% of posts occurring between 2:00 and 10:00 UTC. Notably, Telegram discussions appeared 0–4 hours before official announcements in 69% of the incidents attributed to Telegram (mean lead time: 2.3 hours). Engagement analysis revealed a quality-reach trade-off, with visual summaries achieving 3.2× higher per-message engagement than high-volume text aggregation. Geopolitical signals concentrated in @Russian_OSINT during Russian-nexus events.

Keywords: cybersecurity, temporal pattern analysis, anomaly detection, threat intelligence, Telegram, social media analysis, early warning systems

Keywords: cybersecurity, temporal pattern analysis, anomaly detection, threat intelligence, Telegram, social media analysis, early warning systems

Methods at a Glance

- Dataset: 9,415 messages collected from 9 public Telegram channels over a full year

- Data processing: summaries of daily, hourly, and weekly combined data; calculated 7-day rolling averages as baselines after a 14-day setup period

- Detection approach (using three methods):

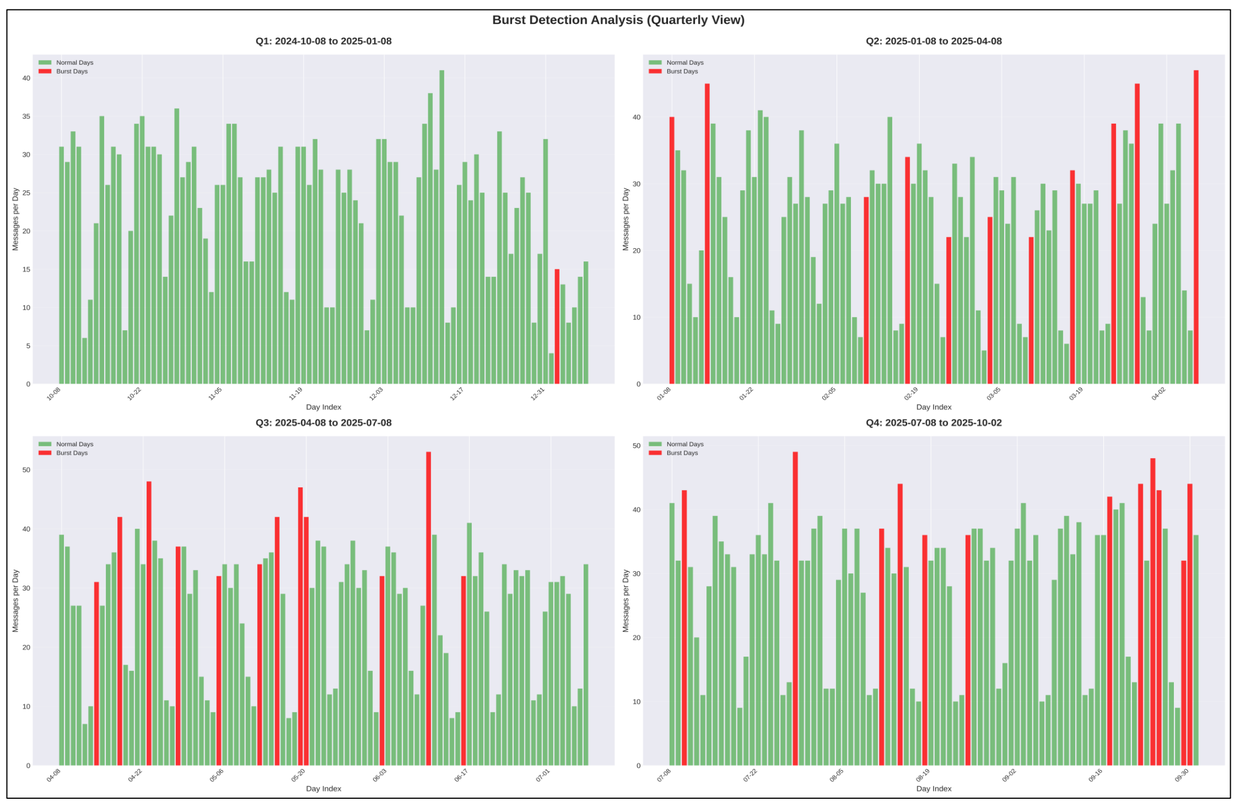
- Z-score: flagged when the absolute Z-value exceeded 2.0 for message counts, views, or forwards
- Percentage change: marked spikes of 50% or more compared to separate weekday/weekend baselines
- Combined scoring: composite score above 4.0 with at least two metrics showing elevated activity

- Verification: automated web searches followed by manual confirmation against CVE databases, official advisories, and news reports

- Statistical reporting: measured effect sizes using Cohen's d, eta-squared, and correlation coefficients; provided 95% confidence intervals through Fisher z-transformation; applied false discovery rate correction for exploratory analyses

- Timing analysis: compared the Telegram activity that occurred with when official advisories were published.

Figures



Key Findings

101 days showed unusual activity (28.1% of the year)

- Successfully linked 80% of the top 10 activity spikes to specific cyber incidents

- Early warning capability: 69% of identified incidents appeared on Telegram 0–4 hours before official announcements (average 2.3 hours earlier, with a standard deviation of 2.8 hours)

- Time-based trends: 52.8% of activity occurred on weekdays (moderate effect size with Cohen's d = 0.38, 95% CI [0.15, 0.61]); 62.1% of posts happened between 2–10 AM UTC; January accounted for 33.7% of all anomalies

- Seasonal variation: month of year explained 14.6% of activity variance (highly significant at $p < 0.001$)

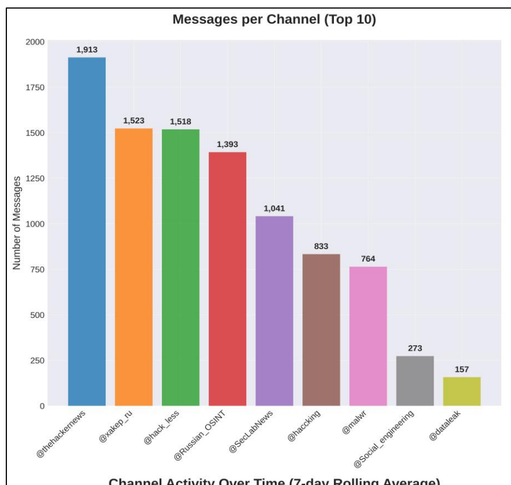
- Weekend pattern: 71.3% of weekend anomalies reflected decreased activity rather than spikes

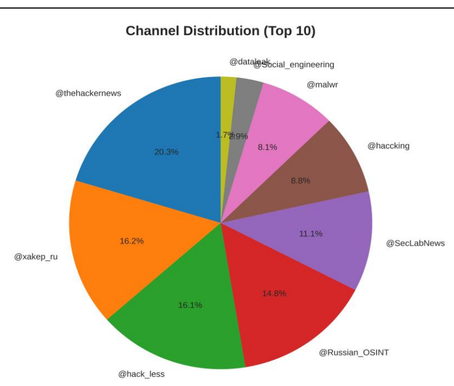
- Engagement trade-off: concise visual summaries generated 3.2 times more engagement than lengthy text compilations (moderate negative correlation of $\rho = -0.42$, 95% CI [-0.50, -0.33])

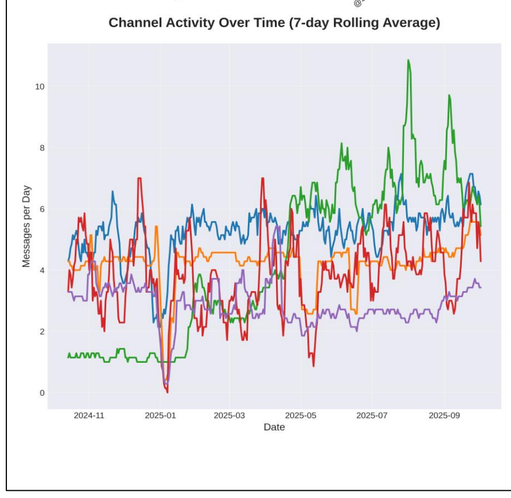
- Geopolitical signal: @Russian_OSINT channel activity strongly correlated with Russian-related cyber incidents (strong correlation of $\rho = 0.78$, 95% CI [0.74, 0.82], $p < 0.001$)

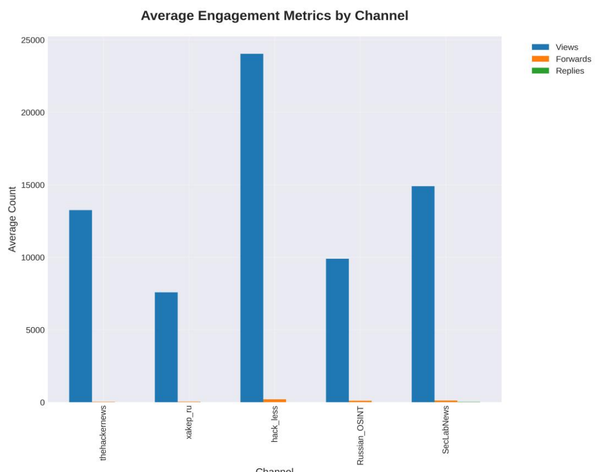
Table: Top 5 Anomalies (Severity & Attribution)

RANK	DATE	SEV.	VIEWS	TOP CHANNEL	ATTRIBUTION
1	2025-01-08	7.07	728,583	@Russian_OSINT (62.3%)	PowerSchool breach + 4 incidents
2	2025-01-24	4.62	1,132,868	@Social_engineering (16.6%)	Apple CVE-2025-24085 zero-day
3	2025-06-10	4.14	612,552	@hack_less (41.0%)	Albemarle ransomware
4	2025-01-09	4.01	386,261	@thehackernews (25.8%)	PowerSchool aftermath
5	2025-01-01	3.97	61,555	@thehackernews (64.2%)	New Year's Day suppression









CONCLUSIONS

- Telegram serves as a quantifiable early-warning system for cyber incidents, typically providing 0–4 hour advance notice for 69% of attributed events (mean lead time: 2.3 hours), validated through 80% attribution success for top-10 anomalies.

- Weekend anomalies primarily represent reduced activity (71.3%) rather than incident surges; interpret these as operational patterns related to staffing and coverage unless multiple metrics and evidence support an actual incident.

- The @Russian_OSINT channel shows a strong association with Russian-linked incidents ($\rho = 0.78$, 95% CI [0.74, 0.82]); valuable for monitoring geopolitical cyber risks and state-nexus operations.

- Temporal patterns reveal structural characteristics of cybersecurity discourse: weekday concentration (Cohen's d = 0.38), January clustering (33.7% of anomalies), and early UTC posting windows (62.1% between 02:00–10:00), with monthly variation explaining 14.6% of activity variance.

The results offer a solid, evidence-based foundation for incorporating Telegram monitoring into security operations. However, practical implementation guidelines and demonstrated reliability across different detection settings are still needed. This approach transforms raw social media data into actionable threat intelligence, delivering measurable and replicable benefits for real-time threat assessment and mitigation.