Proceedings of the 5th International Conference on Interdisciplinary Humanities and Communication Studies
DOI: 10.54254/2753-7064/2026.36252

How Transnational Digital Platforms Respond to Trust Crises under National Security Narratives: The Case of TikTok

Kaiyi Yan

Department of Global Political Economy, The Chinese University of Hong Kong, Hong Kong, China
yankaiyi@link.cuhk.edu.hk

Abstract. This paper uses TikTok as an example to examine how national security narratives shape transnational digital platform trust crises. The research focuses on the controversies on TikTok in Sino-US media and political debate, analyzing how cross-border data flows, algorithmic recommendation, platform ownership and geopolitical tensions translate into public concerns regarding risks and legitimacy. The empirical basis is a preliminary content analysis on 51 news reports published by six Chinese and American media outlets between 2022 and 2025. The study encoded three dominant frames: security threats, business competition, and technological innovation, as well as five information source types: government, business, experts, the public, and international sources. This study employed descriptive statistics, cross-tabulation analysis, chi-square tests, exploratory logistic regression, and case studies to identify key narrative patterns. The results show that security frames dominate the sample, particularly in US media, and that government sources are closely related to security frames. This paper argues that TikTok's trust criss stems from geopolitical securitization, elite information source dominance, technological opacity and the users and creators' invisibility. Future research should expand the corpus, improve inter-coder reliability and compare TikTok with other politically controversial platforms.

Keywords: TikTok, Platform Governance, National Security Narratives, Media Framing, Source Dependence

1. Introduction

TikTok is a transnational digital platform with global user base and strong influence on cross-cultural communication and digital business. Its content dissemination capability and commercial value have made it beyond a common social platform, but a significant platform in digital economy and international communication. However, because TikTok involves cross-border data flows, algorithmic recommendation and platform ownership issues, it has become a controversial object in Sino-US media and political debates, especially around privacy, cross-border data flow and platform governance [1]. In these debates, TikTok is not only described as a social media app, but also a potential national security risk. It has brought trust crises for TikTok and also other transnational digital platforms, because public perception of the platforms is often shaped by political narratives, media strategy and source selection.

© 2026 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

DOI: 10.54254/2753-7064/2026.36252

Therefore, this paper examines how does the trust crisis of transnational digital platforms arises within the context of national security narratives. To answer this question, this paper examines media coverage of TikTok in the United States and China. This paper does not explore whether TikTok is objectively safe but rather focuses on analyzing how TikTok is constructed to appear credible or untrustworthy through specific frames and information source structures. This shift is crucial because platform trust is not merely a technical attribute; it is also a state of public discourse, influenced by factors such as the platform's definers, the risks emphasized, and which voices are highlighted or marginalized.

Existing research has explored TikTok from the perspectives of data sovereignty, national security, platform regulation, and media discourse, but often in isolation. This paper integrates these dimensions, revealing how platform governance issues gain public significance through national security narratives, and how unequal access to information in media reports reinforces these narratives. Through a combination of preliminary content analysis and case studies, this paper constructs a frame arguing that TikTok's trust crisis is not merely a regulatory or technological controversy, but rather a discursive process influenced by geopolitical context, media production, and institutional authority.

2. Literature review

This paper brings together three bodies of literature: transnational platform governance, securitization and national security narratives, media framing and source dependence. First, literature on transnational platform governance explains why platforms like TikTok are ambiguous on technology and institutions Second literature on securitization and national security explains how this ambiguity translates into public concerns about national vulnerability, foreign influence and national security. Third, literature on media framing and source dependence explains how these security implications are selected, disseminated and reinforced in coverage. Therefore, they help explain why TikTok's trust crisis should not be understood only as a technical or legal controversy, but rather as a platform legitimacy crisis resulting from the interplay of factors such as geopolitical interpretation, technological opacity, media framing and source hierarchy.

2.1. Transnational platforms and governance ambiguity

Digital platforms are not only commercial agencies or tools for communication. Nowadays, they are becoming new infrastructures of public communication, playing dominated roles in data flow, market access and cultural visibility. This is especially obvious in transnational platforms, because they run across many different jurisdictions and rely on big data push, algorithmic recommendation and cross-border governance arrangement. As Fenwick, McCahery and Vermeulen argue, platforms challenge traditional enterprise governance pattern because they are not traditional enterprises with clear organizational structures [2]. They operate through Internet, algorithmic management, decentralized participation and continuous experimentation. These characteristics make it hard for platforms to regulate through traditional governance frames designed for companies which are more stable. Zuboff's concept of surveillance capitalism argues how platform enterprises extract behavioral data and convert them into predictive products, creating new forms of asymmetrical knowledge about users [3]. As for transnational platforms, technological opacity and jurisdictional ambiguity are closely linked. A platform such as TikTok is simultaneously a private company, a cultural space, a data infrastructure, a creator economy, and a geopolitical object. Its ownership structure, data practices, and algorithmic recommendation system are therefore not interpreted in a

DOI: 10.54254/2753-7064/2026.36252

neutral environment. When platforms' operation becomes difficult to see, and their commercial characters crosses national boundaries, public trust is likely to be influenced by competing political narratives. Research gaps remain in explaining how platform governance ambiguity is converted into public distrust. Existing research has paid more attention to the difficulties of platform governance, but not how these difficulties are shaped as trust crises by public.

2.2. National security narratives and platform securitization

The second part concerns securitization and national security narratives. Securitization theory argues that the reason why that issue becomes a security problem is not only it has own material character, but also it is publicly constructed as threats which require exceptional attention and intervention [4]. Recent policy and academic discussions argue that securitization is especially evident in debates about whether TikTok will foster foreign influence, expose user data to external actors, or shape the information environment through opaque algorithmic recommendation systems [5]. Cristiano and Monsees further point out that TikTok has become a core issue in the EU and US digital sovereignty debates, where concerns about foreign interference, platform regulation, and cross-border data flows are closely linked to broader disputes over technological sovereignty [6]. These studies support the view that TikTok's trust crisis is not only a matter of platform compliance, but also a product of geopolitical discourse in which data, algorithms, and ownership are redefined as national security issues. Securitization changes the meaning of platform governance, the data governance problem becomes a data sovereignty problem, the algorithmic transparency problem becomes a potential manipulation issue, and the company ownership problem becomes a foreign control issue. Once the transformation happens, the core problem is not only how to regulate the platform, but whether the platform can be trusted. The research gap is the study of platform securitization. While securitization studies tend to focus on how these issues are constructed as security threats, they pay less attention to how media and information source mechanisms stabilize these security implications at the public level.

2.3. Media framing, source dependence, and platform trust

The third part concerns media frames and source dependence. Framing theory provides a method to analysis how media constructs public issues through choosing and emphasizing some parts of reality. Entman first defines frames as a process which selects some parts of reality and makes them more salient in communication [7]. In the later research, Entman further argues that frames can define problems, diagnose the causes, make moral judgements and suggest solutions [8]. This frame is directly relevant to coverage about TikTok, since the coverage not only shows controversies around the platform, but also defines what kind of problem TikTok is, who should response to it, whether the platform is legitimate or dangerous, and which policy response is appropriate. Chong and Druckman argue that frames are not only textual labels, but also a structure which can shape public perception on social issues [9]. Van Gorp's concept about frame package is also useful, since it encourages researchers to look beyond isolated keywords and examine boarder cultural and argumentative ways to construct meanings [10]. Recent research on TikTok further shows that media framing plays an important role in shaping public reception on the platform. Miao et al. examine media coverage regarding TikTok in China, the US, and India, showing a shift from the de-politicisation to the re-politicisation of TikTok This suggests that the platform is interpreted beyond a commercial success or cultural entertainment [11]. Tran et al. focus on media framing and public attitudes toward TikTok bans on a state level, arguing that national security and freedom of speech

DOI: 10.54254/2753-7064/2026.36252

influence public evaluations of the ban [12]. These studies support this paper's argument that TikTok's trust crisis stems not only from technological uncertainty or governance challenges but also from media narratives.

This research analyzes coverage regarding TikTok through three main frames: security threat, business competition and technological innovation. These categories show different ways of defining this platform. Security threat frame treats TikTok as a risk to national security, data sovereignty and public order. Business frames interpret the controversy through market competition and enterprise strategy. Technological innovation frame presents TikTok as a symbol of digital innovation, algorithmic ability or cultural globalization.

However, frame is not just a matter of language. This is also a problem of source structure. Gans believes that news production tends to rely on agency-approved sources because they are accessible, authoritative and compatible with the news routine [13]. The impact hierarchy methods of Shoemaker and Reese further show that news content is formed by multiple levels of influence, including professional routines, organizational constraints, institutional relationships and a broader political environment [14]. These insights are very important for this article, because the trust crisis of TikTok depends not only on the way the platform describes it, but also on who is allowed to define it. Government officials, regulators, courts, experts, company representatives, users and creators have no equal power in media narratives.

Source code dependence is particularly important in security-related platform disputes. When government and expert sources dominate reporting, the explanation of national security may seem more authoritative and less controversial. The platform is in a defensive position when the company's voice appears mainly in response to the allegations. When users and creators are less obvious, the daily social value of the platform is marginalized. Therefore, trust is mediated through the level of voice. The public not only accesses TikTok as a technology; it also contacts TikTok through the narrative organization of institutions, sources and frames.

This article integrates these documents into a simple analytical frame. Transnational platforms are institutionally ambiguous and technically not transparent. The national security narrative can turn this ambiguity into doubt. The media frame organizes the platform as a security threat, business competitor or technologist. Source dependence determines whose interpretation becomes authoritative. Together, these processes have led to a crisis of platform trust. The frame guides empirical analysis by focusing on four mechanisms: geopolitical securitization, the dominance of elite sources, technological opacity, and the implicitness of users and creators. There is still a research gap in linking the media frame with the source structure. Existing studies often analyze media frames and news sources separately, which leads to a lack of in-depth understanding of how their interactions shape public trust in politically controversial platforms. This article aims to fill the research gap by studying how a specific frame-source combination builds TikTok into a security risk, business entity, technology platform or socially significant space.

3. Case, data and method

This paper adopts a case study approach supported by a pilot content analysis on media coverage regarding TikTok. TikTok is selected as the central case because it represents a transnational digital platform. It operates across national boundaries, depends on large scale data processing and algorithmic recommendation, and has become deeply embedded in debates over platform governance, digital sovereignty and Sino-US technological competition. These features make TikTok a useful case for examining how national security narratives generate trust crises for transnational platforms and how such platforms may attempt to rebuild legitimacy.

DOI: 10.54254/2753-7064/2026.36252

This paper's empirical basis is a preliminary content analysis of 51 news articles related to TikTok published by six Chinese and American media outlets between 2022 and 2025. The sample includes 28 articles from US media and 23 from Chinese media. The selection of these media outlets was not random but rather employed a structured comparative logic. Within each national context, this study selected one political media outlet, one business media outlet, and one technology media outlet: for the US, The New York Times, The Wall Street Journal, and Wired magazine; and for China, People's Daily, 21st Century Business Herald, and 36Kr. This design is not intended to represent the complete media systems of both countries, but rather to capture differences in media biases and examine whether different frames exist for TikTok reporting in politics, business, and technology.

The article selection method involved searching for the keyword "TikTok" on the official websites of the aforementioned six media outlets. Search results were sorted by relevance, and the most relevant articles were reviewed to determine inclusion. Inclusion criteria included articles that were centered on TikTok and contained a clear dominant narrative frame related to security threats, business competition, or technological innovation. Exclusion criteria included articles that only mentioned TikTok incidentally, lacked a recognizable narrative frame, appeared as brief news briefs, newsletters, weekly summaries, or reprinted material, or could not be categorized into any of the three analytical frames mentioned above. Therefore, the final sample prioritized articles that actively constructed TikTok as a political, economic, or technological object, rather than those that merely provided brief factual updates. This sampling strategy was suitable for pilot studies because its goal was not to measure the total amount of TikTok coverage, but rather to identify key framing patterns and information source structures within the media narratives surrounding the platform. This paper codes according to 2 dominated dimensions, dominated frame and source type. Dominated frame mains the main narrative logic that how the article defines TikTok as a public issue. This paper uses 3 dominated frames based on the coding scheme which is developed for the pilot study. These three frames are used in this study because they correspond to the three main dimensions of public discourse surrounding TikTok: national security, business competition and technological capability. Furthermore, they are the most stable and easily distinguishable narrative categories in the pilot sample. The first one is security threat frame, which shapes TikTok as a risk to national security, data sovereignty, public order or ideological security. It usually emphasizes problems regarding data leakage, foreign government influence opaque algorithms, surveillance and the need for restrictive regulation. The second frame is business competition frame, which interprets TikTok through market competition, corporate rivalry regulatory barriers and industrial policy. The third one is technological innovation frame, which shapes TikTok as a case that shows digital innovation, algorithmic capability and global cultural communication.

In addition to these frames, this paper also codes the source type of each article. The paper identifies 5 types of sources, including government sources, company sources, expert sources, public sources and international sources. The theoretical basis for this classification stems from Gans' concept of institutional source dependence and Shoemaker and Reese's hierarchy of influence theory [13, 14]. This classification not only examines how TikTok was constructed but also examines whose voices were given authority in shaping the platform into a security risk, a market player, a technological object, or a social space. The government sources include officials, regulators, legislatures, courts and other state institutions. The company sources include TikTok, ByteDance, competing platform companies, industry representatives and corporate spokespersons. The expert sources include scholars, researchers, legal analysts, think tanks and professional commentators. The public sources include ordinary users, content creators, social media participants and individuals. And the international sources include foreign government, international

DOI: 10.54254/2753-7064/2026.36252

organizations, foreign media and transnational institutions. This source classification is important because the paper treats trust crises as both governance problems and narrative problems. Media coverage does not simply report platform controversies; it also organizes public understanding by deciding whose voices are treated as authoritative. When government and expert sources dominate coverage, national security interpretations may become more legitimate and difficult to contest. When public users and creators are less visible, the everyday social value of the platform may be marginalized. Source structure is therefore analyzed as one mechanism through which platform legitimacy is constructed or undermined.

The pilot content analysis is used in an exploratory rather than population-generalizing sense. The sample size is limited and cannot represent all U.S. and Chinese media coverage of TikTok. However, it provides useful evidence for identifying recurring mechanisms through which TikTok's trust crisis is narratively produced. Descriptive statistics and cross-tabulations are used to examine the distribution of frames and source types across countries and media categories. A simple logistic regression is used as exploratory evidence to examine whether national context and government sources are associated with the use of the security threat frame. These quantitative results are supplemented by illustrative case analysis, comparing selected U.S. and Chinese articles to show how similar national security disputes can be narrated through different source structures and legitimacy claims.

To strengthen the methodological contribution of the paper, this study also proposes a small computational extension based on the existing coding scheme. The three frame categories can be operationalized as a dictionary-assisted framing measure. Keywords associated with security, business, and technological innovation narratives can be used to calculate frame scores in a larger corpus of news articles about TikTok. For example, terms such as "national security" "data security" "surveillance" "foreign influence" and "ban" may indicate security framing, while terms related to market competition, monetization, acquisition, and platform economy may indicate business framing. Terms such as "algorithm" "recommendation system" "AI" and "innovation" may indicate technological framing. This computational component is exploratory and is intended to supplement, rather than replace, interpretive framing analysis. Its purpose is to show how a manually developed coding scheme can be extended into a scalable text-analysis frame for future research.

Overall, this method includes interpretive case analysis, pilot content analysis, descriptive statistics and a proposed dictionary-based computational extension. It can help to explain how TikTok's trust crisis is produced through national security narratives, media source structures and platform governance concerns, offering possible response strategies for transnational digital platforms.

This study has several limitations. First, the sample size is relatively small. The analysis is based on 51 news reports related to TikTok from six US and Chinese media outlets; therefore, the results should be considered exploratory rather than representative of the overall media environment in both countries. Second, this study focuses solely on TikTok. While TikTok is a prime example of a transnational platform trust crisis, other platforms may be influenced by different ownership structures, regulatory pressures, user bases, and geopolitical environments. Third, this study is highly time sensitive. Discussions related to TikTok evolve with legal rulings, policy negotiations, platform responses, and broader US-China relations. Therefore, the results reflect the specific period from 2022 to 2025, rather than a stable or final model of platform security.

Future research can address these limitations in several ways. For example, a larger corpus could be constructed, incorporating more media outlets, longer timeframes, and more diverse report types. Computational text analysis could also be combined with manual coding to examine whether the

DOI: 10.54254/2753-7064/2026.36252

framing patterns identified in this pilot study are prevalent on a larger scale. Comparative studies could further examine whether similar trust crises exist on other multinational platforms (such as WeChat, Telegram, X, or Meta-owned platforms). Finally, future research could incorporate user interviews, creator perspectives, or survey experiments to examine how media framing and information source structures influence public trust beyond news content.

4. Findings

In this section, the paper explains how TikTok's crisis is caused through media frames, source structures and platform governance. The analysis shows that distrust is not only direct reaction to technology risks, but also the result of narratives and institutions. Four mechanisms are especially important: geopolitical securitization, elite source dominance, technological opacity and user invisibility.

4.1. Empirical overview

The pilot content analysis shows that security framing is the dominant way in which TikTok is represented in the sample. According to Table 1, among the 51 TikTok-related articles, 33 articles adopt the security threat frame, accounting for 64.71% of the sample. The business competition frame appears in 14 articles, or 27.45%, while the technological innovation frame appears in only 4 articles, or 7.84%. This distribution suggests that TikTok is more frequently narrated as a risk object than as a commercial competitor or technological innovator.

Table 1. Overall frame distribution

Frame type	Count	Percentage
Security threat frame	33	64.71%
Business competition frame	14	27.45%
Technological innovation frame	4	7.85%
Total	51	100%

The cross-national pattern is even more revealing. According to Table 2, among the 28 U.S. media articles, 24 use the security threat frame, accounting for 85.71%. The remaining 4 use the business competition frame, and none are coded as primarily using the technological innovation frame. By contrast, Chinese media coverage is more dispersed: among the 23 Chinese articles, 9 use the security threat frame, 10 use the business competition frame, and 4 use the technological innovation frame.

Table 2. Country × frame distribution

Country	Security threat	Business competition	Technological innovation	Total
China	9/39.43%	10/43.38%	4/17.39%	23
United States	24/85.71%	4/14.29%	0/0%	28

The chi-square test of independence was used to examine the association between country and frame type. The chi-square statistics were calculated as:

DOI: 10.54254/2753-7064/2026.36252

$$\chi^2 = \sum \frac{(O_{ij}-E_{ij})^2}{E_{ij}} \tag{1}$$

O_{ij} refers to the observed frequency in cell i, j of the country-by-frame contingency table, and E_{ij} refers to the expected frequency in the same cell under the assumption that country and frame type are independent. The subscript i represents the country category, and j represents the frame category.

The effect size was measured using Cramér's V coefficient, calculated as:

$$V = \sqrt{\frac{\chi^2}{N(k-1)}} \tag{2}$$

χ^2 refers to the chi-square statistic, N refers to the total number of articles in the sample, and k refers to the variable with fewer categories. In this study, $N = 51$ and $k = 2$ because there are two categories for countries/regions.

The chi-square test shows a statistically significant association between country and frame type: $\chi^2 = 13.025$, $df = 2$, $p < .01$, with Cramér's $V = 0.505$. This indicates a medium-to-strong association between national media context and how TikTok is framed. The U.S. coverage is highly concentrated around security risk, while Chinese coverage combines counter-securitization, business competition, and technological legitimacy narratives.

According to Table 3, source distribution also matters. Across the sample, company sources and government sources are the two most frequently cited categories, appearing 44 and 43 times respectively. Expert sources appear 36 times, international sources 29 times, and public sources 22 times. Public sources, including ordinary users and content creators, are therefore present but comparatively less visible than institutional actors.

Table 3. Source type distribution

Source type	Frequency	Percentage
Company sources	44	25.29%
Government sources	43	24.71%
Expert sources	36	20.69%
International sources	29	16.67%
Public sources	22	12.64%

Finally, an exploratory logistic regression was used to examine whether country and source type are associated with the use of the security threat frame. The model estimates the probability that an article uses the security threat frame. The model is as follows:

$$logit(P_i) = ln[\frac{P_i}{(1-P_i)}] = \beta_0 + \beta_1 US_i + \beta_2 Government_i \tag{3}$$

$$+\beta_3 Company_i + \beta_4 Expert_i$$

DOI: 10.54254/2753-7064/2026.36252

In this model, P_i represents the probability that article i adopts the security threat frame. The dependent variable is coded as 1 if the article uses the security threat frame, and 0 otherwise. $logit(Pi)$ represents the log odds that the article adopts the security threat frame, and $ln[Pi/(1-Pi)]$ represents the natural logarithm of those odds. US_i is a country dummy variable, code d as 1 for articles from US media and 0 for articles from Chinese media. $Government_i$, $Company_i$ and $Expert_i$ are information source type dummy variables, coded as 1 when the article cites the corresponding type of information source, and 0 otherwise. β_0 is the intercept, while β_1, β_2, $\beta_3$and β_4 are the estimated coefficients for country, government, company, and expert sources, respectively.

The dependent variable is whether an article uses the security threat frame. The independent variables include country, government source, company source, and expert source. According to Table 4, the results show that U.S. media are significantly more likely to use the security threat frame $\beta = 2.2844$, $p = .010$. Government source presence is also a significant predictor of security framing $\beta = 3.4826$, $p = .009$. Company sources and expert sources are not statistically significant in this model.

Table 4. Logistic regression predicting security threat frame

Variable	Coefficient	p-value
Country: U.S. media	2.2844	.010
Government source	3.4826	.009
Company source	1.0721	.348
Expert source	0.8991	.277

Because the sample size is limited, these regression results should be interpreted cautiously. They do not prove a causal relationship between government sourcing and security framing. However, they do suggest that security framing is not randomly distributed. It is associated with both national media context and the presence of government sources. This pattern provides the empirical basis for the four mechanisms discussed below.

4.2. Geopolitical securitization

The first mechanism is geopolitical securitization. In usual discussion on platform governance, data protection, algorithmic transparency, ownership structure and content moderation are seen as regulation or technological issues. However, in TikTok's case, these problems are always redefined as national security issues. Therefore, TikTok is no longer a social media service, commercial actor or technological platform, but a potential risk to national sovereignty, data security and information autonomy.

This kind of transformation changes the basic frame of public debate. When TikTok is treated as national security threat, the core question is no longer whether the platform follows privacy rules or market regulation, but if it is worth trusting. Platform ownership becomes a sign of political vulnerability, cross-border data flow becomes possible channels of surveillance and algorithmic recommendation becomes potential influence tools. Even the platform's popularity can be explained as influencing capacity but not cultural success.

A U.S. report on the Supreme Court's review of the TikTok ban provides a useful example of this mechanism [15]. Although the article is formally about the legal debate over whether a TikTok ban

DOI: 10.54254/2753-7064/2026.36252

or forced divestment is constitutional, the platform is repeatedly situated within a national security frame. TikTok is represented as a foreign-controlled technology platform whose data practices may create security risks. The legal issue is therefore inseparable from the political question of whether a Chinese-owned platform can be trusted in the U.S. information environment.

This case illustrates how platform governance becomes securitized. The article does not primarily ask how TikTok's recommendation system works, how users experience the platform, or how the company might improve compliance. Instead, it places TikTok within a frame of national vulnerability and foreign adversary risk. In this frame, regulatory measures such as banning, divestment, or stricter oversight appear not only as policy options, but as protective responses to a possible threat.

The descriptive statistics show that this is not an isolated case. Security framing accounts for nearly two-thirds of the whole sample and dominates U.S. coverage. This suggests that TikToks trust crisis is produced not only by its technical features, but by a geopolitical environment in which those features are interpreted through suspicion. The same features that might otherwise be discussed as platform governance issues (data storage, algorithmic recommendation, ownership, and content circulation) are reorganized as signs of strategic risk.

However, it doesn't mean security concerns are invented or irrelevant. Cross-border data governance and algorithmic accountability are reasonable public issues. The problem is that securitization narrows the range of explanation. Once TikTok is defined as security threat, its commercial role, technological innovation, producer economy and cultural function are no longer as visible as before. The platform is no longer understood as complicated digital infrastructure with multiple meanings, but something that should be limited, regulated or distrusted.

4.3. Elite source dominance

The second mechanism is the dominance of elite. National security narratives are powerful not only because some words which relate to risk appear in coverage, but also because these words are attached to authoritative speakers. Sources can not only offer information, but also help define the problem, assign responsibility, evaluate risk and imply possible solutions in the coverage. For a politically contested platform like TikTok, who speaks is very important to construct trust or distrust.

The pilot analysis shows that government, company and expert sources are more visible than public sources. Government sources appear 43 times while expert sources appear 36 times. And public sources appear 22 times. The logic regression further shows that government sources are strongly associated with the use of security threat frames. However, it doesn't mean government sources will mechanically cause security framing. But it does suggest that security narratives are highly connected to official and institutional forms of speech.

The New York Times article on the Supreme Court reaffirms this information source structure [15]. The narrative is centered on official and legal institutions, including government lawyers, Supreme Court judges, the Ministry of Justice and the presidential powers. These institutions define the TikTok platform as a potential national security risk and debate the legitimacy of restrictive policy responses. TikTok's own voice and the voice of its creators have become more passive or marginalized. Therefore, this article builds a relatively closed explanation structure: the state defines the risk, the legal institution assesses the risk, and the platform needs to solve the risk.

This structure creates asymmetric legitimacy. Government and legal institutions are portrayed as guardians of public interests, while TikTok is censored. Even if the company explains its data governance or legal compliance, these explanations are still evaluated within the security frame built

DOI: 10.54254/2753-7064/2026.36252

by these institutions. TikTok participates in this narrative unequally. It seems to be the defendant, not the co-creator of the public's understanding of the problem.

A Chinese business technology report on TikTok's temporary recovery from the U.S. ban crisis also provides a useful comparison [16]. This article also responds to the ban crisis in the United States and does not avoid security disputes. However, it uses a broader source structure to organize its narrative, including official company statements, expert comments, public reactions and international media coverage. In this narrative method, TikTok is not only a potential security target, but also a company facing political pressure, a platform supported by users, and a symbol of China's digital globalization.

The comparison between The New York Times and 36Kr does not mean that one report is neutral while the other is political. On the contrary, it shows that the structure of the information source will affect the scope of interpretation of the platform. If the security narrative is mainly dominated by official and legal sources, it limits the identity of TikTok to the area of risk and state protection. On the other hand, the more diverse information source structure combines the commercial, public and international dimensions, thus expanding the scope of the narrative. In both cases, the choice of source determines what kind of platform TikTok is allowed to be in public discourse.

For multinational platforms, this has caused serious communication problems. If the platform is mainly discussed through politicians, courts, regulators and security experts, its public identity will be shaped by risks before the platform has the opportunity to explain itself. Public communication becomes passive rather than active. Company statements, compliance promises, or transparency reports may then be interpreted as self-defense rather than credible evidence. In this sense, trust crisis is also a crisis of narrative authority: the platform loses the ability to define the conditions under which it should be trusted.

4.4. Technological opacity

The third mechanism is technological opacity. It's difficult for ordinary users and external observers to evaluate TikTok's data practice, ownership structure and algorithmic recommendation, which makes the platform more likely to be questioned. Things that are hard to observe or verified are likely to be defined as potential risk in the securitized context.

The core technological problem in TikTok controversy is cross-border data flow and algorithmic recommendation. Data flow causes problems about where users' information is stored, who has access to the information and whether national actors can get access to it or influence the use of it. Algorithmic recommendation leads to another concern, whether the platform's content distribution system can shape attention, visibility, or political perception in ways which are difficult to be detected by users. These problems are not unique to TikTok. Many global platforms rely on massive data extraction and opaque recommendation systems. However, the geopolitical status of TikTok creates these problems of special security significance.

This mechanism is reflected in the security threat frame itself. The coding scheme regards data leakage, foreign government control, opaque algorithms and information manipulation as key elements of the security frame. In other words, technological non-transparency is not only a background condition, but also one of the elements that constitute the basis of the narrative of TikTok's trust crisis.

A U.S. report on Nebraska's lawsuit against TikTok shows useful boundary cases for understanding technological opacity [17]. This article is not included in the main three-frame sample, because it focuses more on youth protection, platform harm and algorithm addiction than security, business competition or technological innovation. However, it still illustrates how

DOI: 10.54254/2753-7064/2026.36252

algorithmic opacity becomes a flexible source of skepticism. In this case, the focus is not on external control, but on the potential harm that the system may cause to minors. Narrative logic is similar: because algorithms are difficult to observe and evaluate externally, their impact is usually interpreted as risk. Its relevance to this article is that it believes that TikTok's algorithm recommendation system is difficult to observe, evaluate and investigate responsibility from the outside. This supports the view that when the platform algorithm is still not transparent, uncertainty turns into public doubt. In the field of national security, doubt is often related to foreign influence or data control.

This case helps to clarify the broader mechanism. The opacity of the algorithm does not necessarily lead to the narrative of national security. It can also support descriptions of consumer protection, youth safety, mental health or moral supervision. However, in the controversy on TikTok, geopolitical tensions make it easier to incorporate technological uncertainty into the discourse of security. The same recommendation system can be described as a tool for personalization, creativity and interaction, or as a tool for manipulation or influence.

A wider range of samples reinforces this. Among the 51 articles, only 4 articles used the technological innovation frame. In addition, 37 articles do not mention the technological innovation frame at all. Even commercial and technical media often adopt security or commercial competition frames instead of emphasizing TikTok's algorithms or technical achievements. This shows that once TikTok becomes the focus of political controversy, its technology is unlikely to be described as innovative and is more likely to turn into a problem of risk, control or market conflict.

Therefore, the lack of transparency of technology exacerbates the crisis of trust; even if the evidence is incomplete, distrust seems reasonable. Doubt persists, and the platform does not need to prove direct causal damage. Its complexity is enough to attract people's attention. If users and reporters do not know where the data is stored, who can access them, or how to recommend the system to organize visibility, political actors and media narratives will define these systems for them.

4.5. User and creator invisibility

The fourth mechanism is user and producer invisibility. TikTok's public meaning is not only constructed by government, courts, companies and experts, but also by daily practices of use, such as entertainment, cultural expression, enterprise promotion, education and creator labor. However, these dimensions are always marginalized in national security narratives. Users are no longer seen as active participants in digital culture, but more as passive objects which are possibly influenced, manipulated or exposed to data risks.

The source distribution supports this point. Public sources appear less frequently than companies, government, and expert sources. This means that ordinary users, platform creators, and social media participants are present in the coverage, but they do not occupy the same level of narrative authority as institutional actors. Their visibility is limited, and their role is often secondary.

The New York Times Supreme Court article demonstrates this pattern. TikTok creators are relevant to the legal dispute because a ban would directly affect them, but they do not define the central problem of the article. The main interpretive authority belongs to state and legal actors. Users and creators appear as affected parties, not as actors who can define what the platform means socially, culturally, or economically. The platform is therefore discussed mainly from above: as an object of state protection, legal judgment, and national security evaluation.

The 36Kr article offers a contrasting narrative arrangement. It gives more space to public reaction, user discussions, and the platform's broader social meaning. In this narrative, TikTok is not

DOI: 10.54254/2753-7064/2026.36252

only a company facing U.S. regulatory pressure. It is also a platform with users, cultural visibility, and symbolic value in global digital communication. This does not make the article free of political framing. But it shows that when users and public reactions are included, the platform is harder to reduce to an abstract security threat.

When user and creator perspectives are marginalized, public debate becomes detached from the communities most directly affected by platform governance decisions. Bans, forced divestment, regulatory restrictions, or algorithmic reforms are then discussed primarily as matters of state security or corporate compliance, rather than as decisions with social and economic consequences for users. It weakens platform's legitimacy. And the national security narratives occupy a dominated role because other meanings which relate to the platform are limited.

5. Conclusion

These four mechanisms show that TikTok's trust crisis is not only caused by a single controversy or single technological character but comes from a boarder narrative structure. Geopolitical securitization turns platform governance into a national vulnerability problem. Elite sources dominance provides security narratives with institutional authority. Technological opacity makes uncertainty distrust. User and producer invisibility keeps platform's daily value away from the center of public debate. These findings are meaningful to platform response strategies, although they don't provide a policy model. The contribution of this research is to connect platform governance to media frames and source analysis. The research shows that platform trust is not only a technological character, and it can not only be protected by compliance. Trust is also the result of narrative and institution structure. And for transnational platforms which operate under geopolitical tension, their legitimacy depends on not only how they govern data, algorithmic and content, but also how they construct public meanings in the media system. Future research can expand this polit study through expanding the corpus, applying dictionary-assisted computational frame analysis and comparing TikTok with other transnational platforms facing similar security narratives.

References

[1] Su, C., & Tang, W. (2023). Data sovereignty and platform neutrality – A comparative study on TikTok's data policy. *Global Media and China, 8*(1), 57-71.

[2] Fenwick, M., McCahery, J. A., & Vermeulen, E. P. M. (2019). The end of 'Corporate' governance: Hello 'Platform' governance. *European Business Organization Law Review, 20*, 171–199. https://doi.org/10.1007/s40804-019-00137-z

[3] Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. https://cds.cern.ch/record/2655106

[4] Otukoya, T. A. (2024). The securitization theory. *International Journal of Science and Research Archive, 11*(1), 1747-1755.

[5] Lewis, J. A. (2024). TikTok and national security. *Center for Strategic and International Studies*.

[6] Cristiano, F., & Monsees, L. (2025). Beyond the ban: TikTok and the politics of digital sovereignty in the EU and US. *Politics and Governance, 13*. doi: 10.17645/pag.10461

[7] Entman, R. M. (1993). Framing: Toward clarification of a fractured paradigm. *Journal of Communication, 43*(4), 51–58. https://doi.org/10.1111/j.1460-2466.1993.tb01304.x

[8] Entman, R. M. (2004). *Projections of power: Framing news, public opinion, and U.S. foreign policy*. University of Chicago Press.

[9] Chong, D., & Druckman, J. N. (2007). Framing theory. *Annual Review of Political Science, 10*(1), 103–126. https://doi.org/10.1146/annurev.polisci.10.072805.103054

[10] Van Gorp, B. (2006). The constructionist approach to framing: Bringing culture back in. *Journal of Communication, 57*(1), 60–78. https://doi.org/10.1111/j.0021-9916.2007.00329.x

DOI: 10.54254/2753-7064/2026.36252

[11] Miao, W., Huang, D., & Huang, Y. (2023). More than business: The de-politicisation and re-politicisation of TikTok in the media discourses of China, America and India, 2017–2020. *Media International Australia, 186*(1), 97–114. doi: 10.1177/1329878X211013919
[12] Tran, H. D., Diep, P. P. U., & Booth, H. (2025). National security versus freedom of speech: How media exposure, personal values, and media framing influence non-users' support for a national ban on TikTok. *New Media & Society*. Advance online publication. doi: 10.1177/14614448251349427
[13] Gans, H. J. (1979). Deciding what's news: A study of CBS Evening News, NBC Nightly News, Newsweek, and Time. http://ci.nii.ac.jp/ncid/BA06385513
[14] Shoemaker, P. J., & Reese, S. D. (1995). Mediating the message in the 21st century: A media sociology perspective. https://ci.nii.ac.jp/ncid/BB1394787X
[15] Liptak, A. (2025). Supreme Court seems poised to uphold law that could ban TikTok in the U.S. *The New York Times*. https://www.nytimes.com/2025/01/10/us/politics/supreme-court-tiktok-ban-law.html
[16] Huashang Taolüe. (2025). TikTok fuhuo beihou de shengsi shisu [The life-or-death race behind TikTok's revival]. *36Kr*. https://36kr.com/p/3167862838897157
[17] De Avila, J. (2024). Nebraska sues TikTok for allegedly harming minors. *The Wall Street Journal*. https://www.wsj.com/us-news/nebraska-sues-tiktok-for-allegedly-harming-minors-5826c533