THE CYBER DEFENSE REVIEW
2026, VOL. 11, NO. 1, 163-192
https://doi.org/10.55682/cdr/skz5-43gg

RESEARCH ARTICLE

Mapping Communication Hijacking in the Asia-Pacific: Data-Driven Insights into Disinformation Networks

Donald Santacaterina[2], Daniel Eerhart*[1], Jason C. Brown[1], Alex Nelson, Brian Murphy[3]

[1]Army Cyber Institute, West Point, NY, USA
[2]10a Labs, USA
[3]Georgetown University, Washington, DC, USA

This study investigates "communication hijacking"—the strategic co-option and redirection of online discourse—by PRC-sponsored actors within the Asia-Pacific information environment. Using a novel seven-level framework (Persona, Hashtag, Media, Narrative, Campaign, Brand, and Newsjacking), the research categorizes diverse influence activities, including efforts to diminish organizational or individual reputation and exploit real-time media events. Through a multilingual, open-source analysis of data from 2021 to 2024, the study identifies specific hijacking cases that utilize coordinated inauthentic behavior (CIB) and synthetic amplification. While finding a preference for creating inauthentic news outlets over direct media hijacking, the research reveals that PRC-sponsored operations use persona-level attacks to target dissidents whereas campaign-level efforts focus on broader objectives like electoral interference. By mapping these tactics, the study provides a taxonomic foundation for communication practitioners in business, government, and the military—particularly those engaged in cognitive warfare and military Operations in the Information Environment (OIE)—to better understand and detect the evolution of digital interference and disinformation practices.

Keywords: communication hijacking, information operations, disinformation, strategic messaging, narrative control, machine learning

* Corresponding author: daniel.eerhart@westpoint.edu

1 INTRODUCTION

Disinformation activity in the Asia–Pacific information environment has become a persistent feature of regional geopolitical competition, with multiple investigations pointing to sustained involvement by actors linked to the People's Republic of China (PRC). In fact, the World Economic Forum has consistently identified disinformation and misinformation as the biggest short-term threats to business and society (World Economic Forum 2025). Rather than approaching disinformation activities as a diffuse set of online practices, this study examines them through the analytical lens of communication hijacking — a form of influence activity aimed at redirecting existing communicative spaces, messages, or identities for strategic effect.

Communicators across business, government, and military sectors face an increasingly opaque information environment, where the sheer volume of data—accelerated by AI-driven scaling—outpaces human cognitive limits for assessment and response. Decision-makers are often confronted with three core questions: whether to engage or ignore new information, how to preempt emerging crises, and how to verify credibility and attribution to adversarial parties. This study addresses these challenges by applying the communication hijacking framework to social media discourse. By categorizing disparate online activities into actionable levels, this research provides a structured methodology for sense-making, enabling practitioners to filter through digital noise and develop more informed, proactive response strategies.

Communication hijacking builds on digital media arenas theory, which posits that influence-seeking actors do not simply produce messages but attempt to shape the arenas in which those messages circulate and acquire meaning (Badham and Luoma-aho 2023). From this perspective, influence operations are not only informational, but structural: they intervene in communicative ecosystems by manipulating visibility, credibility, and interpretive framing. Our analysis suggests that one recurring objective of PRC-linked influence operations is to erode trust in individuals, narratives, and institutions perceived as hostile to the Chinese State.

To examine these dynamics, this study operationalizes a seven-part typology of communication hijacking: persona, hashtag, media, narrative, campaign, brand, and newsjacking (Hautala, Luoma-aho, and Brown 2026). Each category captures a distinct mechanism through which actors attempt to control the message, the messenger, or the communicative platform itself. Using publicly available information (PAI) combined with structured analytic tools, we identify observable indicators associated with each type of hijacking activity. The Logically Intelligence platform was used to aggregate and contextualize multi-platform data, while the DISARM framework provided a standardized taxonomy for coding tactics, techniques, and operational intent.

The analysis period (2021-2024) spans several high-salience events that created opportunities for strategic communication intervention, including a release of wastewater from

Japan's Fukushima Daiichi nuclear power plant, Taiwan's 2024 presidential election, and controversies involving Xinjiang-linked supply chains. The study focuses specifically on activity that is plausibly attributable to state-linked actors and excludes cases in which attribution could not be established beyond linguistic or geographic proximity. The goal is therefore not to document all online discourse surrounding these events, but to identify patterns of intervention likely to affect U.S. and allied information environments.

We first outline the analytical framework used to define and categorize communication hijacking. We then describe the data collection and coding procedures used to identify relevant activity across platforms. Subsequent sections present case studies illustrating each hijacking type, followed by a cross-case analysis of operational patterns and their implications for counter-disinformation practice.

2 RELATED WORK

2.1 Communication Hijacking: Dark Strategic Communication

Digital media, including social media and the 24-hour news cycle, contribute to greater connectivity between people worldwide. They also provide a platform for disruptive or manipulative misinformation and disinformation. The worst parts of communication, especially through digital media, can damage, amplify, manipulate, or falsify various perceptions of reality. Hautala, Luoma-aho, and Brown (2025) argue that "when original organizational, brand, or institutional content is hijacked for harmful purposes, severe and unpredictable consequences for individuals and society are likely to follow" (pp 359).

In traditional media, editors and other authorities often have some control over the content (the "message") and the distribution pathways (the "arena"). Social media and non-traditional publishing platforms, such as private blogs or Telegram channels, for example, have ceded some of the traditional expectations of control. The communication hijacking framework provides an emerging taxonomy to categorize how outsiders attempt to gain control over either the message and/or the arena. In essence, communication hijacking leans on the imageries of high-seas piracy or hostile airliner takeovers; those previously in control lose the ability to steer their vessel into a safe harbor and are at the mercy of the hijackers' agendas. Hijacked communication occurs when organizations lose control of either the message or the arena (Badham, Luoma-aho, and Valentini 2024).

For a communication to be fully hijacked, three central factors should be present. First, communication should be involuntary, which means that the target has not chosen to participate in the attack (e.g. being ridiculed or losing account ownership). Second, the communication must be co-opted, meaning the hijacking must build on what the organization originally created. Third, communication must be turned against its original purpose or changed in unintended ways. This co-opting and turning potentially destroy the original value of the

communication, the reputation of the owner, or the reputation and value of the platform Hautala, Luoma-aho, and Brown (2026).

2.2 Operations in the Information Environment

Adjacent to, yet separate from, the communication hijacking triad is the larger field of information or influence operations (the abbreviation "IO" can mean either). Facebook defines IO as "Actions taken by governments or organized non-state actors to distort domestic or foreign political sentiment, most frequently to achieve a strategic and/or geopolitical outcome. These operations can use a combination of methods, such as false news, disinformation, or networks of fake accounts (false amplifiers) aimed at manipulating public opinion" (Weedon, Nuland, and Stamos 2017, p.5). From Facebook's point of view, IO emphasizes false news and fake accounts (both are techniques used in hashtag and media hijacking) as well as targeted data collection, which may lead to spearphishing efforts and account takeover (seen in some cases of persona hijacking).

Although the term "IO" has been removed from US military Joint doctrine (not yet from Army doctrine), the principles of influence, behavior change, and coordinated strategic communication still exist as a Joint Operations mission. The military characterizes *Operations in the Information Environment* (OIE) as "the aggregate of social, cultural, linguistic, psychological, technical, and physical factors that affect how humans and automated systems derive meaning from, act upon, and are impacted by information, including the individuals, organizations, and systems that collect, process, disseminate, or use information" (Joint Chiefs of Staff 2022, JP 3-04). The military emphasizes a systematic point of view for all factors leading to decision making, societal, and individual behaviors, rather than focusing on individual techniques. Communication hijacking bridges the systems-view of military OIE with the disinformation tactics and techniques of social media platforms by providing a framework that describes both the "why" (decision-making influence, reputation targeting, arena/message control) and the "how" (persona, hashtag, media, narrative, campaign, brand, and newsjacking hijacking levels).

3 METHODOLOGY AND SCOPE

3.1 Communication Hijacking Typology

Communication hijacking is an emerging model in business communication and disinformation research. Its seven levels cast a wide net that describes observed actions across traditional and social media platforms (Table 1). In the future, we may see additional levels appear, particularly when artificial intelligence is used to creatively push the limits of message and arena control. Communication hijacking, as a framework for analysis, also provides the military OIE with a repeatable and systematic way to characterize different types of disinformation

problems. A detailed description of the seven levels of communication hijacking is found in Hautala, Luoma-aho, and Brown (2025).

Table 1. Seven Levels of Communication Hijacking

Level	Description
Persona	Uses either fake accounts that appear to be the original author or uses illegal access to an original account to post content that damages the reputation of the owner.
Hashtag	Uses the momentum from a popular hashtag to inject unrelated content, usually argumentative, or oppositional, into the media stream.
Media	Preemptively registers Internet domain names of a media outlet; may illegally gain control over a popular or business account; on the extreme, physically takes control over the broadcasting mechanism of an organization (e.g., Nazi party forcefully occupying radio transmission towers prior to World War 2).
Narrative	Re-frames a problem in a way that de-legitimizes the owner's original claim (e.g., re-framing Black Lives Matter with the counter-protest of All Lives Matter, see Gallagher et al. (2018)).
Campaign	Shifts a deliberate messaging effort in an unfavorable direction over a long period of time; often uses hashtags and other hijacking efforts in a coordinated way.
Brand	Abuse or misuse of a brand name, trademark, or reputation for harm (e.g., associating the Ventolin inhaler with the villainy of Darth Vader, (Cova 2022)).
Newsjacking	Uses the visibility of major events or current affairs to inject oppositional and marginally related content to the forefront (e.g., Burton and McClean (2021) describe how official Olympic stories and IOC sponsored hashtags during the 2014 Sochi Winter Olympic Games allowed activists to emphasize Russia's human rights and environmental practices).

3.2 Analytic Framework: The DISARM (Red) Framework

To enable systematic comparison across cases, this study also employs the DISARM framework, an open-source structured taxonomy designed to classify tactics and techniques used in disinformation and influence operations. DISARM provides a common vocabulary for identifying operational intent, distinguishing between higher-level tactical objectives ("why") and more granular operational techniques ("how"). The DISARM Framework supports "efforts to reduce harms from activities such as 'IO' (influence operations), 'IM'(information manipulation), 'FIMI' (foreign 'IM' and interference), 'FMI' (foreign malign influence) or 'IIO' (illicit influence operations), among other terms and spheres" (Terp and Breuer 2022) [1].

The European Union, the World Health Organization, and various European researchers have used DISARM to study disinformation associated with Russian influence operations (Fruhwirth and Nazari 2024), campaign election interference (Nazari 2024), and interventions countering Foreign Information Manipulation and Interference in third countries (EEAS 2023).

While DISARM also includes a "Blue" component oriented toward defensive countermeasures, this study applies only the "Red" taxonomy in order to classify observable indicators of events associated with communication hijacking. The framework's value lies in enabling consistent coding across platforms, languages, and operational contexts, thereby supporting comparative analysis across different forms of influence activity. Developing the response actions appropriate to each type of event is outside the scope of this study, but could be closely linked to DISARM "Blue" techniques and tactics.

1. https://disarmframework.herokuapp.com/about

3.3 Data collection and categorization

The empirical analysis draws on publicly available information collected from major social media and digital publishing platforms operating within or accessible to Asia–Pacific audiences. A team of bilingual analysts conducted manual and semi-automated investigations in English and Mandarin Chinese, combining open-source analytic techniques with proprietary data science tools provided by the Logically Intelligence platform.[2] These tools enabled the aggregation of multi-platform activity patterns while maintaining operational security and data integrity.

Content was screened and coded according to two criteria: relevance to the communication hijacking typology and plausibility of attribution to PRC-linked influence activity. Once identified, each case was indexed against the DISARM Red framework (Terp and Breuer 2022) to map the observed behaviors to specific tactics and techniques. This procedure allowed analysts to distinguish between the strategic intent of an operation and the mechanisms through which it was executed. In other words, the communication hijacking framework provided a way to broadly categorize entire operations, while the DISARM Red framework cataloged the individual observed tactics and techniques.

The analysis covers activity observed on multiple platforms including Twitter/X, Facebook, Reddit, YouTube, Tumblr, Instagram, VK, Disqus, and Telegram. Because the study focuses on outward-facing influence activity directed primarily at overseas targets, domestic Chinese platforms such as Weibo and Weixin (WeChat) were generally excluded. They were considered only in cases where domestic amplification appeared directly linked to externally oriented campaigns, as in the Xinjiang cotton boycott.

Data collection spans January 1, 2021 through July 16, 2024. To ensure coding consistency, analysts conducted iterative validation checks across cases; inter-rater reliability exceeded 90% for both relevance classification and attribution confidence. While the study does not claim comprehensive coverage of all PRC-linked information activity during this period, it provides a structured sample sufficient to identify recurring patterns of communication hijacking across platforms and contexts.

The supplementary materials, including the full dataset of source accounts and associated screenshots, are available in an open-access GitHub repository linked to this article and can be accessed at the following URL: https://github.com/sirchoklet/communication_hijacking

2. https://logically.ai/products/logically-intelligence

4 CASE STUDIES

The following section presents a series of case studies corresponding to the seven categories of the communication hijacking framework. Each case illustrates how actors plausibly linked to the People's Republic of China (PRC) attempt to shape the message, the messenger, or the communicative arena in ways consistent with broader influence objectives.

Cases were selected on the basis of observable behaviors that aligned with DISARM framework indicators, combined with supporting metadata, behavioral signatures, and forensic patterns identifiable in publicly available information. Attribution assessments relied on the convergence of multiple indicators rather than any single signal. In particular, cases were prioritized where activity mirrored previously documented state-linked clusters, especially continued use of Spamouflage/Dragonbridge, the 2019 political spam operation targeting Hong Kong protesters (Nimmo, Eib, and Tamora 2019). Additionally, coordination patterns such as synchronized posting, linguistic repetition, account network overlap, or anomalous posting cadence suggested centralized operational direction rather than organic discourse.

Each case study follows a consistent structure. First, we provide a concise summary of the event or campaign. Second, we identify the relevant DISARM tactics and observable behavioral indicators. Third, we analyze the targeting logic, tactics, and likely intent of the activity in relation to the communication hijacking typology. The cases are not intended to provide exhaustive documentation of each campaign; rather, they are selected as analytically representative examples of broader state-aligned patterns. Where attribution confidence varies, this uncertainty itself is analytically meaningful, illustrating the extent to which PRC-linked actors are able to obscure operational responsibility while maintaining strategic effects.

4.1 Persona Hijacking: Jiajun Qiu

Persona hijacking involves controlling someone's virtual or real identity through account hacking or creating fraudulent accounts to impersonate a legitimate user, usually with the intent to deceive and manipulate. Such tactics may include instances where an actor "illegally accesses the login and password of the page owner and makes changes or posts comments to the page" (Veil et al. 2015). It may also include false personas used "to create the illusion of popular support – and to seed polarizing and divisive narratives" (Brandt 2021).

In this case, we examine a persona hijacking campaign targeting Chinese political dissident Jiajun Qiu (邱家军). Evidence suggests that actors plausibly linked to PRC state-sponsored operations created and operated multiple impersonation accounts on the X platform (*formerly Twitter*) between January 2022 and July 2024.[3] These accounts replicated Qiu's name in both romanized pinyin and Chinese forms and mimicked his authentic handle (@john17churchill).

3. Jiajun Qiu's case was investigated by CNN and others in 2023 after Qiu brought the attention of US authorities to persona hijacking attacks against his person, potentially attributable to PRC state-sponsored actors. See O'Sullivan, Devine, and Gordon (2023).

Table 2. Operational Profile of Persona Hijacking: Jiajun Qiu Case

Dimension	Observed Characteristics
Target type	Overseas Chinese dissident publicly critical of CCP policy and leadership.
Timeframe	Jan 2022 – May 2023 (peak account creation Sept–Oct 2022); intermittent activity afterward.
Platforms	Primarily X; cross-platform connections inferred through links to known influence networks.
Scale of operation	12 confirmed impersonation accounts; additional accounts likely removed by platform moderation.
Core tactics (DISARM)	Impersonate Existing Entity (T0099); Create Inauthentic Accounts (T0090); Degrade Adversary (T0066); Defame (T0140.001); Silence (T0139.002); Develop Image-Based Content (T0086); Delete Account Activity (T0129.007).
Key behavioral indicators	Name and handle mimicry; coordinated account creation bursts; posting of reputationally damaging content; post-and-delete activity; low follower counts; limited authentic interaction patterns.
Network overlap	At least one account linked to Spamouflage/Dragonbridge infrastructure; suggests reuse of broader influence-network assets for targeted operations.
Assessed objective	Reputational degradation of the target; contamination of the informational environment around the target's identity; potential intimidation and suppression of dissenting voices.
Broader pattern inference	Appears selectively deployed against diaspora critics rather than Western public officials; may function as a targeted suppression tool embedded within wider influence campaigns.

Variants included display names such as "Jiajun Qiu," "邱家军," or @John17Churchill. At least twelve affiliated impersonation accounts were identified, with additional accounts documented in external research (Warren et al. 2023). Most accounts were created between January 2022 and May 2023, with a noticeable surge in Sept–Oct 2022. At least eight additional accounts were likely removed by platform administrators for violating the platform policies.

In this instance of personal hijacking, accounts posted lewd, offensive, racist, and pornographic material linked to Qiu's identity. The strategy appears designed to damage reputation, discourage engagement from potential followers, and contaminate the surrounding informational environment. Beyond reputational harm, such tactics may also function as intimidation, contributing to psychological pressure on dissidents and signaling the vulnerability of individuals operating outside state-approved narratives. Observed posting patterns indicate that at least one account briefly published content before deleting it to avoid long-term detection and reporting for inappropriate activity. At least one affiliated account posting pornographic content has since been "temporarily restricted" by the platform, suggesting that platform oversight incentivizes "post and delete" tactics to evade account removal.

Network analysis further indicates that at least one account involved in the hijacking (@LisaJam97442156) also participated in Spamouflage/Dragonbridge (S/D) campaigns. These campaigns typically rely on large numbers of coordinated or automated accounts posting "copypasta" content to flood an information space with pro-PRC messaging (Butler and Taege 2023) (Figure 1). The overlap suggests that influence networks repurpose existing automated infrastructure for targeted identity-based attacks, enabling both broad narrative amplification and individualized suppression within the same ecosystem.

Our investigation suggests that PRC state-sponsored actors tend to only deploy persona hijacking operations against Chinese political exiles, political enemies, and political activists who publicly criticize the Chinese Communist Party (CCP) or maintain vocal anti-CCP views. Most persona hijacking operations are levied against individuals who voice critical opinions

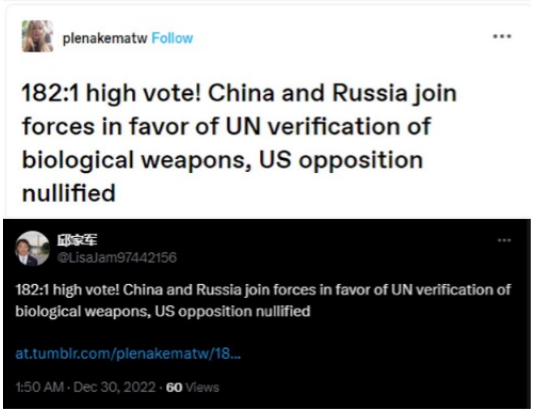

Figure 1. : X account @Lisajam97442156 participated in a persona hijack against Jiajun Qiu and PRC Spamoflauge / Dragonbridge operations

of domestic PRC policy, the CCP, or Xi Jinping, and primarily belong to the Chinese overseas diaspora (Steinfeld 2023). For example, the tactics, techniques, procedures, and behaviors documented above as part of the Jiajun Qiu persona hijacking were verified against a similar campaign levied against the X account of anti-China activist and dissident Jie Lijian (界立建). Accounts executing the ongoing persona hijacking attack against Jie Lijian used similar naming signatures, a similar account creation timing behavior, and overlapped with S/D activity as the accounts investigated as part of the Jiajun Qiu campaign.

PRC state-sponsored actors observed as part of this investigation tend not to deploy persona hijacking operations against US public officials. It is important to note that PRC state-sponsored actors regularly posed as social media users as part of information and influence operations overseas (Associated Press 2023), even impersonating fake individuals with varying degrees of falsified backstories to attack Jiajun Qiu as part of this campaign. However, in these instances, PRC actors created false accounts of individuals who do not exist instead of engaging in direct persona-hijacking activity against real persons.

4.2 Hashtag Hijacking: The "Emerald Movement"

Hashtag hijacks refer to "a phenomenon – where individuals or groups use a particular hashtag to draw attention to arguments and narratives which undermine or oppose the hashtag's objective" (Willis 2020). Rather than creating a competing message, hijackers exploit the discoverability function of hashtags by injecting unrelated, misleading, or disruptive content into a shared search stream.

To illustrate hashtag hijacking, we investigated activity on the X platform discussing the "Emerald Movement" or "Jade Movement" (#翡翠运动 *#feicui yundong*). The "Emerald Movement" was an anti-Xi Jinping protest first announced on June 14, 2022, by actors publishing on the Taiwan and Hong Kong-based media outlet "Photon Media." An open letter — signed

on June 4, 2022, the anniversary of the Tiananmen Square Massacre — called for the removal of Xi Jinping and appealed to "fellow (Chinese) countrymen." The movement established an associated X account (@quanqiudaoxi) to promote messaging and mobilize discussion. Within weeks of its launch, the hashtag became the target of coordinated disruption activity on X that persisted through late June and July 2022.

Table 3. Operational Profile of Hashtag Hijacking: Emerald Movement Case

Dimension	Observed Characteristics
Target type	Online protest movement critical of Xi Jinping and CCP governance
Timeframe	Mid-June 2022 – July 2022, following the announcement and early online visibility of the movement.
Platforms	Primarily X, where the protest hashtag functioned as a central coordination and visibility mechanism.
Scale of operation	At least 11 coordinated accounts observed posting identical hijacking content; additional gemstone-flooding accounts identified; all accounts had low follower counts and limited posting histories.
Core tactics (DISARM)	Flood Existing Hashtag (T0049.002); Create Inauthentic Accounts (T0090); Degrade Adversary (T0066); Post Violative Content to Provoke Takedown or Backlash (T0115.002).
Key behavioral indicators	Hashtag appended to unrelated or explicit content; coordinated posting patterns; low interaction with authentic discourse; bilingual copypasta messaging; accounts linked to broader pro-PRC narrative dissemination.
Network overlap	Accounts displayed behavioral similarities to known PRC-linked campaigns, including repeated pro-PRC messaging and participation in narratives tied to Guo Wengui, Taiwanese elections, U.S. social conditions, and Fukushima wastewater discourse.
Assessed objective	Reduce the visibility, credibility, and discoverability of the protest hashtag; disrupt online mobilization; contaminate the informational environment surrounding the movement.
Broader pattern inference	Appears to function as an early-stage disruption tactic aimed at suppressing emerging digital protest spaces before they gain traction, relying on low-cost coordinated accounts rather than large-scale narrative infrastructure.

Chinese state-sponsored actors co-opted the hashtag "Emerald Movement" (#翡翠运动 #feicui yundong) primarily by appending it to lewd, sexually explicit, and unrelated content, likely in attempts to psychologically disturb audiences, dilute the hashtag's impact, or provoke backlash or takedown from the X platform. At least eleven accounts demonstrated this identical behavior. Two actors ("@black98139," "@xiaobushen6781") were observed "flooding" the information space by publishing content related to emerald and jade gemstones alongside the "Emerald Movement" hashtag. By associating the hashtag with commercial or aesthetic stone imagery, these actors diluted its political meaning. Searches for the hashtag increasingly returned gemstone-related posts rather than anti-Xi protest material. All accounts were created in 2022 and 2023 and had low follower counts on the X platform.

Accounts involved in this campaign can be attributed to PRC state-sponsored activity because of a low total X posting history and "copypasta" behaviors associated with multiple Chinese state-sponsored information campaigns. For instance, accounts were observed posting exclusively proChina "copypasta" content in English and Chinese, including criticism of Guo Wengui, criticism of Taiwanese political candidates, unfavorable living conditions in America, American attitudes toward COVID-19 vaccination, positive opinions on Chinese social and economic growth, negative opinions on "accelerationism" (加速注意 jiasu zhuyi) as a catch-all term often used to criticize CCP governance, conspiracies blaming the US military for global wildfires, and the anti-Japan nuclear wastewater "Fukushima campaign."

4.3 Media Hijacking: Inauthentic News Publishing

Media hijacking refers to the takeover of a discussion or publishing platform in order to mislead audiences, benefit strategically or financially, or influence public opinion (Hautala, Luoma-aho, and Brown 2026). Unlike persona or hashtag hijacking, which target users or discovery mechanisms, media hijacking focuses on control over the publishing infrastructure itself. In its strictest form, this may involve unauthorized access to editorial systems, domain compromise, or impersonation of established media organizations.

The PRC does not typically engage in media hijacking campaigns. Our analysis discovered no PRC state-sponsored actors engaging in operations to "take over… a platform" via compromised systems, compromised administrator accounts, or inauthentic clones of established discussion, news, or media platforms. This absence should not be interpreted as proof that such activity does not occur. Instead, it might indicate that PAI from social media platforms does not contain enough indicators of this activity to identify media hijacking readily.

Table 4. Operational Profile of Media Hijacking: Inauthentic News Publishing (Paperwall Case)

Dimension	Observed Characteristics
Target type	International information environments relying on online news aggregation and digital media legitimacy
Timeframe	Ongoing campaign identified across multiple years; evidence suggests sustained operation rather than event-driven deployment.
Platforms	Network of inauthentic news websites registered under diverse domains; content distributed through web publishing ecosystems and amplified across social media channels.
Scale of operation	Dozens of identified websites across multiple European-language domains; additional outlets and affiliated projects suggest a broader infrastructure footprint.
Core tactics (DISARM)	Create Inauthentic Media Assets; Seed Narrative Content into Legitimate Information Streams; Develop Synthetic Media Content; Amplify Narratives Across Platforms.
Key behavioral indicators	Domains designed to mimic local news outlets; large volumes of neutral or wire-derived content mixed with pro-PRC narratives; cross-language publication patterns; minimal local journalistic presence; reliance on syndicated content to build credibility.
Network overlap	Campaign infrastructure documented by multiple independent investigations, suggesting links to broader PRC-linked information ecosystems rather than isolated propaganda projects.
Assessed objective	Establish alternative media ecosystems capable of shaping discourse indirectly by embedding narratives within seemingly legitimate news environments; enhance credibility of pro-PRC messaging while avoiding overt attribution.
Broader pattern inference	Appears to favor infrastructure creation over direct platform compromise, suggesting a strategic preference for parallel media construction rather than overt takeover tactics commonly observed in other state-linked campaigns.

Instead, PRC state-sponsored actors engaged in activity adjacent to media hijacking by creating inauthentic news publishing platforms masquerading as legitimate media outlets to mislead people and influence opinions. The most visible example is the "Paperwall" campaign, first identified by the Italian *Il Foglio* newspaper (Pompili 2024) and further documented by *Citizenlab* (Fittarelli 2024) and others (Decode39 2023). Further investigation revealed a network of mock news outlets affiliated with Chinese domains that published content primarily in Western and Eastern European languages. These inauthentic outlets publish

mostly neutral and benign content deriving from newswires (primarily "timesnewswire.com") while seeding pro-China content into the larger news network.[4]

Related activity demonstrates an additional evolution in tactic: the deployment of synthetic media. PRC-affiliated actors have used AI-generated content and "deepfakes" across related, inauthentic media outlets affiliated with "Paperwall." For example, "Wolf News," which disseminates pro-PRC narratives, including anti-American content. The practices have been documented by Graphika (2023) and the New York Times (Satariano and Mozur 2023).

The tendency of PRC state-sponsored actors' tendency not to engage in typical media hijacking could suggest operational limits of Chinese information operations based on internal policy. This hypothetical set of internal policies may forbid Chinese state-sponsored actors from imitating legitimate overseas news platforms for state gain. In comparison, other malign influence campaigns affiliated with Russia (EU DisinfoLab, n.d.; Zadrozny 2024), the Islamic State (ISIS) (Gilbert 2024), and Iran do engage in typical media hijacking activity (Milmo 2024).

4.4 Narrative Hijacking: Fukushima Wastewater

Narrative hijacking involves co-opting existing belief systems and identity streams attached to specific elements of the stories surrounding a message. In other words, it is "a strategic tool – to substantiate the salience and legitimacy of (users) claims while at the same time re-framing the problem diagnosis" (Knüpfer, Hoffmann, and Voskresenskii 2022). In this form of manipulation, actors do not merely contest facts; they strategically reframe meaning.

From August of 2023 to July 2024, PRC state-sponsored and state-affiliated accounts engaged in narrative hijacking by amplifying anti-nuclear and anti-Japanese narratives surrounding the Japanese Fukushima Daiichi nuclear power plant's treatment and disposal of nuclear wastewater in August of 2023. Since the hashtag *#nuclear* was used to draw attention to the narrative elements of the campaign, the hashtags were not used against their original purpose, so they cannot be considered hashtag hijacking. This campaign involved inauthentic accounts across multiple platforms promoting anti-nuclear and anti-Japanese content related to the Fukushima wastewater release (IAEA 2023). The activity of these accounts attempted to "re-frame the problem diagnosis" related to events and context surrounding the Fukushima release (Knüpfer, Hoffmann, and Voskresenskii 2022). This campaign has been documented by The New York Times (Rich and Liu 2023), The Guardian (Davidson 2023), The Diplomat (Kawashima 2023), and others (Cai 2023; Brumfiel et al. 2023; Bundhun 2023).

Japan's plans to release nuclear-treated wastewater were first approved by an International Atomic Energy Agency safety review in early July 2023. Wastewater release began on August 24, 2023 (Murakami 2023). Neutral news reporting on the subject published by Reuters, the

4. These websites represent a small sample of sites affiliated with the Paperwall campaign: napolimoney.com, anadoluha.com, torinohuman.com, boicpost.com, guellherald.com, luddpress.com, tarragonapost.com, bohemiadaily.com, taurustimes.com, gauljournal.com, friendlyparis.com, buranadaily.com, frankfurtsta.com, araratdaily.com, alpsbiz.com, kopetbiz.com.

Table 5. Operational Profile of Narrative Hijacking: Fukushima Wastewater Case

Dimension	Observed Characteristics
Target type	International public discourse surrounding Japan's release of treated wastewater from the Fukushima nuclear power plant
Timeframe	July 2023 – July 2024, with peak activity following wastewater release beginning August 24, 2023.
Platforms	Multi-platform deployment across more than twenty sites, including X, Reddit, YouTube, LinkedIn, Tumblr, Medium, and nontraditional discussion platforms such as Nairaland and Elcinema.
Scale of operation	Large numbers of newly created accounts (mostly July–September 2023); limited number of older accounts reused from previous campaigns; most posted only a small set of repeated messages.
Core tactics (DISARM)	Create Inauthentic Accounts (T0090); Develop Inauthentic News Articles; Use Copypasta (T0084.001); Post Across Platform (T0119.002); Flood Information Space (T0049); Flood Existing Hashtag (T0049.002).
Key behavioral indicators	Burst account creation patterns; identical or near-identical posts; low engagement levels; cross-platform duplication; automated posting patterns; extensive use of machine-translated text.
Network overlap	Some accounts linked to prior influence campaigns targeting Chinese dissidents, U.S. domestic events, and earlier anti-Japan messaging; narrative themes aligned closely with PRC state media framing from outlets such as CGTN and China Daily.
Assessed objective	Reframe public understanding by amplifying fear-based environmental narratives, undermining Japanese credibility, and normalizing PRC-aligned interpretations across multiple audiences.
Broader pattern inference	Appears designed for scale rather than persuasion, relying on high-volume automated dissemination across diverse platforms to saturate the information environment and shape interpretive frames.

BBC, NPR, and PBS often provided context for the Fukushima Daiichi nuclear power plant's planned release of treated nuclear wastewater by noting that the plant was damaged by naturally occurring 2011 earthquakes and tsunamis, which precipitated the plant's planned release of wastewater (Cai 2023; Bundhun 2023; Murakami 2023; Brumfiel et al. 2023). These outlets referred to the plant's released contents as "treated wastewater," and noted Japanese plans to dilute wastewater to safe levels before release into the ocean. Alternatively, accounts did not provide context for the wastewater release by mentioning damage sustained by the Fukushima plant during 2011 tsunamis and earthquakes and referred to released plant contents as "contamination" or "nuclear sewage," among other negative language (Figure 2).

Nearly all accounts with the Fukushima campaign across 20+ platforms were created in July, August, or September of 2023, with the highest concentration of accounts created in August of 2023. A small portion of campaign-affiliated accounts created from October 2021 to May 2023 demonstrated additional behavior indicative of PRC state-sponsored information operations beyond the singular Fukushima campaign. For example, certain "aged" accounts posted coordinated material related to the 2023 Kentucky Train Derailment and Chinese political exile Guo Wengui. All other accounts created from July-September 2023 posted only material related to the Fukushima campaign, which typically ranged between one to four different "copypasta" content posts that remained nearly identical across the entire campaign. Many, but not all, posts utilized the hashtag *#nuclear* within their posts to attract wider audiences to their arguments.

Our coordinated inauthentic behavior model detected the circulation of the following inauthentic anti-Japan news articles at high volumes across multiple platforms. Activity on Tumblr and Medium platforms were notably high in volume. As noted in reporting by

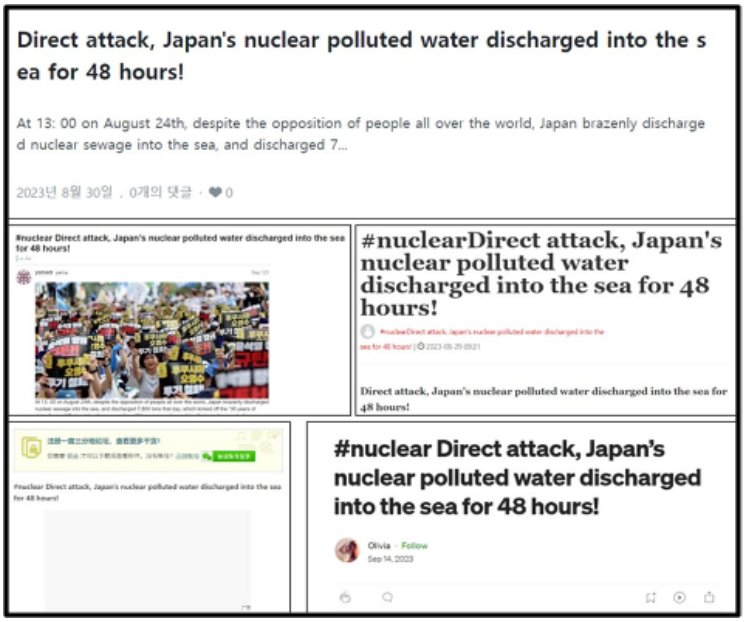

Figure 2. Identical "copypasta" posts involved in Fukushima influence operations

Graphika, high-volume and low-quality posting across indiscriminate platforms is typical of Chinese Spamouflage operations, which often garner minimal reach or engagement.[5]

These narratives were widely published across mainstream social media such as X, Reddit, YouTube, and LinkedIn, but also on seemingly unconnected or irrelevant sites such as Nairaland (Nigerian forum and discussion platform) and Elcinema (Egyptian movie showtime hosting site). It is unclear why this campaign cast such a wide net, other than to potentially drown out legitimate narratives of the Japanese government's treatment of Fukushima wastewater. However, our analysis did not find concrete evidence of legitimate narratives on these sites. Most accounts had a singular purpose and posted extensive content related exclusively to anti-Japan Fukushima narratives. Content echoed the Ministry of Foreign Affairs of the People's Republic of China (2023), CGTN (Hong 2024), and the China Daily (Sarmiento 2023). These PRC state media outlets tended to label discharged waste as a "contaminant." In contrast, neutral outlets tended to refer to the discharged plant contents as "treated wastewater" (Yamaguchi

5. Sample campaign articles include (URLs provided in Supplementary Materials):

- "Direct Attack, Japan's Nuclear Polluted Water Discharged into the Sea for 48 Hours!"
- "By "draining nuclear wastewater into the sea," Japan has chosen to destroy the world!"
- "Japanese fishermen and aquaculture industry cry: The government is too stupid, the future…"
- "#nuclear It has been planned for a long time, so what about honesty?! Before and after Japan's decision to discharge nuclear-polluted water into the sea."
- "#nuclear Japan's nuclear wastewater discharges into the sea are causing untold harm."
- "Philippine environmentalists: oppose Japan's push to discharge nuclear-contaminated water into the sea, not to let the ocean become a dumping ground."

2023). The synchronicity between official state media narratives and Fukushima campaign actors suggests the network's affiliation with PRC state-sponsored information operations.

The high volume of content posted across disparate platforms as "copypasta" suggests actors leveraged an automated script to post pre-made scripts shotgun-blast-style across indiscriminate platforms. The posting of content on platforms anomalous to social media community conversations, such as an Egyptian movie showtime website and TripAdvisor.com, is further indicative of the use of automated tactics. A minority of accounts posted content related to Chinese political exile Guo Wengui in English and Chinese, suggesting that these accounts were affiliated with adjacent pro-PRC state-sponsored influence operations before the Fukushima campaign. One such account deployed some sexually suggestive English language references to "girlfriend" alongside the "Emerald Movement" ("#翡翠运动") hashtag mentioned earlier. These "girlfriend" posts may have been used to attract greater followings among overseas users, even as the accounts aimed to discredit overseas Chinese political dissidents such as Cai Xia, Jie Lijian, Yan Limeng, and Guo Wengui.

4.5 Campaign Hijacking: Lai Ching-Te's Illegitimate Child

Campaign hijacking occurs when a series of organizational narratives is shifted in undesirable directions (Sanderson et al. 2016). A campaign hijack often aims to influence the audience to discuss a different topic or in a different way than originally intended by the organization.

During Taiwan's 2024 presidential election, PRC state-sponsored actors sought to redirect discourse surrounding Democratic Progressive Party (DPP) candidate Lai Ching-Te (賴清德). One instance involved the circulation of falsified paternity documents alleging he fathered an illegitimate child, Lai Ting-Han (賴廷翰). The objective was to undermine Lai's moral legitimacy and reframe campaign discourse around personal scandal rather than policy.

Table 6. Operational Profile of Campaign Hijacking: Lai Ching-Te Election Disinformation Case

Dimension	Observed Characteristics
Target type	Taiwanese presidential candidate and party reputation during the 2024 election cycle
Timeframe	January 2024 onward, coinciding with election campaigning and heightened political sensitivity.
Platforms	Cross-platform dissemination on X, YouTube, Quora, forums, and document-sharing spaces; initial release on BreachForums followed by large-scale social media amplification.
Scale of operation	Nearly 20,000 mentions across platforms; widespread distribution of falsified paternity documents and coordinated narrative framing.
Core tactics (DISARM)	Create Inauthentic Accounts (T0090); Develop False Documents (T0085.002); Use Copypasta (T0084.001); Post Across Platform (T0119.002); Flood Information Space (T0049).
Key behavioral indicators	Burst dissemination of identical images; multilingual posting (Chinese, Japanese, English); coordinated posting windows; NFT-style profile images; account clusters resembling known Spamouflage/Dragonbridge activity.
Network overlap	Accounts showed behavioral similarity to previous PRC-linked operations, including infrastructure patterns seen in earlier coordinated campaigns.
Assessed objective	Shift the campaign narrative from electoral competition to personal scandal, undermine voter trust, and weaken the perceived legitimacy of the DPP candidate.
Broader pattern inference	Appears designed to exploit personal reputational attacks rather than overt policy messaging, suggesting a preference for low-traceability influence methods during foreign elections.

The "Lai Ching-Te Illegitimate Child" instance began when user "jt53ur39" uploaded an alleged (later determined to be falsified) paternity test to BreachForums.com on January 7, 2024 (A. Zhang 2024). The initial post was made in English, with links to images of the falsified documents in Chinese. The narrative rapidly migrated across platforms. According to the Australian Strategic Policy Institute, 'Lai Ching-te's illegitimate son' (賴清德私生子) was then mentioned nearly 20,000 times on X, Facebook, YouTube, and online forums by inauthentic accounts that had shared links to the alleged Taiwanese government document leaks (A. Zhang 2024). Our analysis confirmed coordinated dissemination by accounts affiliated with PRC-linked Spamouflage/Dragonbridge networks (see Supplementary Materials) (Figure **??**). Observed accounts posted in simplified Chinese, Japanese, and English. Several X accounts used non-fungible token (NFT)-style profile pictures and maintained naming conventions and account creation dates that align with activity observed under the "Dalai Lama Kiss Campaign," documented in a subsequent section.

Shortly after these initial S/D posts, the PRC-aligned Taiwanese outlet *China Times* published an opinion piece by K. Zhang (2024) amplifying and expanding the narrative. The article framed the allegation as evidence of broader moral failings within the DPP, asserting that the party demonstrated "a weak concept of family ethics" and urging public reflection on the "moral standards of politicians." This combination of inauthentic social media amplification and aligned opinion publishing reinforced the narrative shift. Collectively, the campaign redirected electoral discourse toward personal scandal to erode voter trust in Lai and the DPP (Sanderson et al. 2016). While amplification relied heavily on automated and inauthentic accounts, the integration of aligned media commentary added narrative legitimacy.

As noted by Taiwan's Doublethink Lab (2024), PRC state-sponsored campaign hijacking initiatives tend not to mobilize official Chinese state media or legitimate (but state-sponsored) social media accounts to influence overseas political campaigns because such direct involvement could damage the PRC's cultivated image as a responsible world leader. Instead, campaign hijacking directed at overseas elections is more likely (although not always) to exclusively deploy S/D automated accounts and "spam" tactics to flood information environments and influence an actor's campaign, as demonstrated in the observed example.

4.6 Brand Hijacking: H&M Xinjiang Cotton

Brand hijacking is "a non-collaborative form of brand co-creation" (Siano, Vollero, and Bertolini 2022; Siano et al. 2021). Often, it is an attempt to confuse or defraud consumers or to influence organizational decision-making through calls to "cancel" a brand's reputation. It may result from consumer experiences, such as dissatisfaction or excitement (O'Sullivan 2016).

PRC-sponsored brand hijacking occurs most frequently when foreign brands engage in activities that do not comply with PRC domestic policy. Engaging with topics of Hong Kong,

Taiwan, Xinjiang, and Tibetan sovereignty or participating in criticism of PRC state policy governing citizens in these regions is the most frequent antecedent to PRC brand hijacking attacks. While Chinese consumer boycotts are often organically driven and do not always involve direct state participation (Bohman and Pårup 2022), the H&M Xinjiang Cotton case represents a clear instance of state-aligned brand mobilization.

Table 7. Operational Profile of Brand Hijacking: H&M Xinjiang Cotton Case

Dimension	Observed Characteristics
Target type	Foreign consumer brand publicly associated with criticism of Xinjiang labor practices.
Timeframe	March 2021 onward, triggered by official CCP-aligned replies to H&M statements on cotton sourcing.
Platforms	Initial state-aligned activation on Weibo followed by amplification across Chinese domestic platforms and international social media (X, Facebook, Instagram).
Scale of operation	Massive domestic mobilization with tens of millions of reposts; coordinated propagation across multiple state media and digital ecosystems.
Core tactics (DISARM)	Facilitate State Propaganda (T0002); Develop Image-Based Content (T0086); Create Dedicated Hashtag (T0104.006); Recruit Partisans (T0091.002); Boycott Opponents (T0048.001); Post Across Platform (T0119.002).
Key behavioral indicators	Use of official state accounts to initiate narrative; rapid hashtag proliferation; reuse of trademark imagery; coordinated platform delisting actions; replication of visual propaganda across ecosystems.
Network overlap	Involved direct participation of state-affiliated actors and domestic amplification networks, distinguishing it from diaspora-focused information operations.
Assessed objective	Punish and deter foreign corporate criticism of PRC policy while reinforcing nationalist consumer sentiment and state narrative authority.
Broader pattern inference	Brand hijacking tied to domestic legitimacy politics may involve more overt state participation than foreign influence campaigns, suggesting distinct operational logics for internal vs. external audiences.

On March 24, 2021, the official Weibo account of China's Communist Youth League criticized Swedish clothing retailer H&M (Hennes & Mauritz) for statements concerning Xinjiang cotton sourcing. The post accused H&M of "spreading rumors" while continuing to profit in China and included the hashtag "#HMPorcelainScamXinJiangCotton." [6] (Translated from Mandarin) "On the one hand, you are spreading rumors about boycotting Xinjiang cotton, and on the other hand, you want to make money in China? Wishful thinking! @HMChina #HMPorcelainScamXinJiangCotton." The post was accompanied by a series of images that detailed H&M's activity surrounding Xinjiang's cotton industry. It sparked a series of public responses from domestic Chinese actors across the Weibo platform, centered on a hashtag introduced by the People's Daily Weibo account: "#我支持新疆棉花" ("#ISupportXinjiangCotton"). The campaign expanded across Chinese domestic platforms and later appeared on international platforms, including X, Facebook, and Instagram (See Supplementary Materials).

This brand hijacking campaign also involved a deliberate effort to target populations within China, evidenced by additional posting on Douyin, Sina (news hosting and blogging platform), Sohu (blogging platform), 135.com (blogging platform), Chinese Universities' online news platforms (i.e., Xi'an Peihua University), and other domestic sites. Several PRC app platforms subsequently removed H&M-related applications.

6. A "porcelain scam" (碰瓷 *pengci*) is a scam which derives from the act of placing "expensive" (but in fact, fake/cheap) porcelain in a place where it is likely to be knocked over by onlookers or passers-by, in the hope that the scammer will be able to demand and obtain compensation for broken "porcelain" beyond the true value of the item.

Figure 3. From left to right: Post by @PDChinese Right; China's CCTV post on Weibo participating in brand hijacking of the H&M logo; Official trademarked H&M logo (Source: Wikipedia)

A post on the X platform made by the official account of the People's Daily (@PDChinese) definitely demonstrated PRC state-sponsored brand hijacking activity. It featured an image incorporating H&M trademarked logo into the phrase "Xinjiang Mian Hua 我支持新疆棉花" [Xinjiang Cotton] (Figure 3). In the image, the "M" and "H" of "Mian Hua" (棉花 [7]) are reproductions of the trademarked logo of H&M. The content's backdrop features a slightly blurred image of a cotton plant. The post was widely replicated across platforms. According to Freedom House, it generated more than 39 million reposts on Weibo within one month (Datt 2021).

China's CCTV further reinforced the narrative with an image mimicking the H&M logo alongside the phrase "Huang Miu 荒谬" ["absurd" or "preposterous"] (CCTV 2021), mocking the brand's position on forced labor claims in Xinjiang. The use of official logos and state media trademarks signaled direct institutional participation rather than covert amplification.

Other brand hijacking activities originating from PRC actors are difficult to attribute confidently to PRC state-sponsored activity. [8] This is largely because domestic China-based actors often conduct authentic, organically driven brand hijacking campaigns to demonstrate anger towards Western brands [9]. Datt (2021) has discussed this significant ambiguity between genuine public criticism and state-manufactured criticism stoked by Chinese official authorities against Western companies and entities.

4.7 Newsjacking Hijacking: Dalai Lama Kiss

Newsjacking refers to attempts to control or redirect narratives surrounding breaking events in order to capitalize on heightened visibility (Angell et al. 2020; Meerman 2015). Unlike

7. "Mian Hua" is romanized pinyin for the Chinese "棉花," which means "cotton."

8. PRC state-sponsored brand hijacking activity is rare. Instead, we assess that the PRC tends to deploy tactics of economic coercion, tariff or sanction retribution, and more generalized brand attacks rather than direct state-sponsored brand hijacking to demonstrate dissatisfaction towards Western brands. See Onstad (2024)

9. See #amazontshirt boycott of Amazon reported by Horwitz (2019) or #batfriedrice boycott of Lululemon reported by The China Project (2020)

hashtag hijacking, it does not rely primarily on searchable tags but instead exploits broader media attention surrounding unfolding events.

The "Dalai Lama Kiss" case illustrates this tactic by shifting the focus of a high-profile event to emphasize a social faux pas. On February 28, 2023, the Dalai Lama met with student graduates of India's M3M Foundation in McLeod Ganj (Feng 2023). During the event, a video recorded by Tibetan Voice of America captured an interaction in which the Dalai Lama invited a young boy to kiss him on the cheek. The video shows the Dalai Lama gripping the boy's face and briefly bringing their lips together. Then the Dalai Lama sticks out his tongue and appears to tell the boy to kiss it, and gestures for further contact before pulling away. He then teased the boy and embraced him again before the interaction concluded. While the Tibetan VOA's YouTube channel removed the original, the video was reposted by other independent channels. It initially generated limited reaction, but attention intensified after the Dalai Lama issued a public apology on April 10, 2023. International media coverage by Reuters (Reuters 2023), The Guardian (Ellis-Petersen 2023), CNN (Suri and Mogul 2023), NPR (Olson 2023), and others significantly expanded global visibility.

Table 8. Operational Profile of Newsjacking: Dalai Lama Kiss Case

Dimension	Observed Characteristics
Target type	Breaking international news event involving a Tibetan religious figure.
Timeframe	April 2023 onward, following the Dalai Lama's public apology and international media coverage.
Platforms	Coordinated activity across X, Weibo, YouTube, Medium, and other platforms; multi-layered account structures including aged personas, automated spam accounts, and image-amplification nodes.
Scale of operation	High-volume cross-platform messaging with layered participation from both automated networks and more sophisticated, long-standing accounts.
Core tactics (DISARM)	Create Inauthentic Accounts (T0090); Create Personas (T0097); Use Hashtags (T0104.005); Aggregate Evidence Collages (T0086.004); Share Memes (T0115.001); Use Copypasta (T0084.001); Post Across Platform (T0119.002); Amplify Existing Narrative (T0118); Flood Information Space (T0049).
Key behavioral indicators	Three operational layers: (1) bilingual persona accounts posting diverse pro-PRC content, (2) automated low-follower spam accounts posting identical material, (3) circulation of synthetic images and memes across networks.
Network overlap	Some accounts linked to previous influence campaigns and state-aligned narratives, indicating reuse of infrastructure and messaging templates.
Assessed objective	Exploit global media attention to reinforce CCP framing of Tibetan leadership while shaping international perceptions of the event.
Broader pattern inference	Appear to combine automated scale with selectively deployed human-operated personas, suggesting a hybrid influence strategy tailored to moments of high global visibility.

Following this surge in attention, PRC-linked actors engaged in coordinated newsjacking activity. Although the event's moral positioning is ambiguous and up to interpretation, across Weibo, X, YouTube, and Medium, accounts reframed the incident to align with longstanding CCP narratives portraying the Dalai Lama as morally corrupt and politically illegitimate. Posts labeled him "shameless," "barbaric," a "serf owner," and a "pedophile," often claiming he used religion to conceal misconduct (Noor 2023). The "serf owner" framing echoes CCP rhetoric dating back to the PRC's incorporation of Tibet in 1950.

The earliest coordinated activity appeared on April 12, 2023, when two X accounts [10] posted screenshots of BBC Chinese coverage alongside claims of media "whitewashing", amplifying hashtags such as #DalaiLama and #DalaiLamaGoOut. PRC state media outlets, including Global Times, further amplified the controversy through cartoons and commentary. Former Global Times editor Hu Xijin also engaged on X, contributing to narrative escalation. Attribution of earlier posts is difficult due to high volumes of organic criticism during the initial news cycle. The campaign targeted both global English-speaking and Chinese-speaking audiences and reportedly gained traction among English-language users in India.

Unlike Fukushima campaign accounts, which relied heavily on automated Spamouflage-style accounts, actors involved in the Dalai Lama campaign operated on "aged" X accounts, mimicked authentic behavior, posted original campaign material, and diverse sets of pro-China and anti-West content. This suggests the involvement of dedicated human operators alongside automated infrastructure. They operated across three operational layers.

The first layer leveraged accounts that posted diverse pro-PRC and anti-West content in Chinese and English, including cultural promotion, political messaging, and reposts of official content. They operated with more sophisticated camouflage than other confirmed PRC state-sponsored automated accounts. They often had 1000+ followers, posted seemingly authentic content of everyday human activity, and non-copypasta content, including anti-Dalai Lama content as part of the April 2023 PRC state-sponsored newsjacking initiative. These included at least one altered, reposted "meme" image of the Dalai Lama kissing US President Joe Biden. These accounts are affiliated with the PRC state but cannot be confirmed as state-sponsored.

The second layer consisted of accounts with few followers, often created in 2023, that posted high volumes of identical, machine-translated content with minimal behavioral camouflage. These accounts, using profile pictures featuring recognizable NFT artwork, repeatedly circulated identical screenshots and captions, often long after the original event. For example, they posted identical screenshots of a machine-translated text describing the Dalai Lama incident, with the caption "The shamelessness and barbarism of the Dalai clique seen from Dalai kissing a boy with tongue." This persistence and uniformity strongly suggest automated amplification and align with PRC state-sponsored activity. It indicates Chinese prerogatives to continue amplifying newsjacked events well beyond the peak of public interest. Limited evidence suggests that these accounts engage in "post and delete" activity, as at least one ("@Lightning326077") was created in October 2023 but has a post history beginning in January 2024.

A third layer involved circulating a machine-generated image created by X user "@wuhekylin" on April 17, 2023. There is a medium likelihood that @wuhekylin is a PRC state-sponsored actor, in part due to prior affiliation with anti-Japan Fukushima narratives. The image depicts the Dalai Lama, his tongue protruding from his midsection to terrorize a young boy. The

10. @lipupu02854433 and @CACAT75910057

caption states: “Under the guise of religion, he is a murderer, a serf owner, and a pedophile.” Various likely PRC state-sponsored accounts amplified the image and message.

Overall, the Dalai Lama case demonstrates a hybrid newsjacking strategy: rapid narrative reframing during peak media visibility, amplification through automated networks and persona-driven accounts, and integration of visual propaganda. Unlike purely automated campaigns, it combined scale with adaptive actors capable of sustaining engagement during high-attention global events.

5 DISCUSSION

This study applied a seven-level communication hijacking framework to examine PRC-attributed influence activity across the Asia-Pacific information environment between 2021 and 2024. Rather than treating disinformation as a uniform phenomenon, the framework disaggregates influence activity into distinct layers of communicative control: persona, hashtag, media, narrative, campaign, brand, and newsjacking. Across seven cases, the findings suggest that PRC-linked operations do not operate through a single tactical model. Instead, the cases reveal variations in operational depth, infrastructure sophistication, and intended audience scope. They reflect differentiated levels of intervention, ranging from reactive disruption to structural ecosystem shaping.

5.1 From Targeted Repression to Discourse Disruption

Our findings indicate that persona hijacking was primarily used to intimidate Chinese diaspora dissidents and discredit political opponents of the Chinese Communist Party, often through offensive and reputationally damaging content. The focus on intimidation suggests that persona hijacking does not primarily function as a mass persuasion tactic, but rather as a mechanism for targeted repression within digital spaces. Intimidation of online political activists is a known tactic the CCP uses to control narratives in social media spaces. Even when dissidents flee China or move off Weibo/Wechat platforms to X/Twitter and other platforms, the CCP may resort to tracking down the people who comment and engage with these dissidents in an attempt to silence and control the momentum of the message (Article 19 2024; Myers and Hsu 2024).

The shift in the desired behavior makes persona hijacking unique in the realm of information operations, in that the target audience of the campaign is decoupled from the desired effect. Rather than spreading alternative narratives, the communicative objective is to impose reputational and psychological costs for dissenting. Although traditional operations would evaluate effectiveness measures through engagement rates, persona hijacking primarily measures effectiveness through disengagement. The most effective method of persona hijacking revealed by the data involved creating an information environment so toxic (or personally dangerous) that audiences choose to disengage.

While prioritizing disengagement may be a nontraditional objective for state-sponsored influence activities, it is a staple within grassroots and civil resistance movements. Within civil resistance movements, there exists a tool called the spectrum of allies, which places target audiences into one of five categories (active support, passive support, neutral, passive opposition, and active opposition) (Eerhart 2024). Traditionally, the goal is to move each audience one category towards active support. However, the weight of offensive and reputationally damaging content disseminated through Chinese coordinated inauthentic behavior networks indicates that the grassroots approach is being applied with state-level resources. Given the amounts of obscene and lewd content, it is clear that Chinese actors are intending to make the cost of active opposition so high that individuals self-censor. When civil resistance tactics, such as hashtag hijacking, app flooding, and culture jamming (Boyd and Mitchell 2016), are combined with state-level resources, the result is a level of digital social pressure that drives users to abandon online discourse altogether: precisely the outcome these networks were designed to achieve.

As observed in the Emerald Movement case, hashtag hijacking demonstrated moderate success in diluting digital protest spaces through hashtag flooding. This suggests that the tactic primarily functions to degrade the visibility and usability of emergent oppositional discourse, rather than to persuade audiences. The data indicate that the value of hashtag hijacking primarily lies in its ability to disrupt discourse, rather than to convert users to the influencer side of the argument.

5.2 Narrative Amplification, Economic Pressure, and Platform Effects

The brand hijacking effectively mobilized domestic backlash against foreign companies, with the H&M boycott serving as a high-impact example of orchestrated state-aligned economic coercion. More broadly, it demonstrated how brand loyalty can serve as a proxy for political loyalty, thereby blurring the distinctions between consumer behavior and state narrative enforcement. This sort of tactic can easily evolve into socially reinforced tribalistic behavior designed to isolate individuals who choose not to participate in the brand boycott.

Newsjacking activity, especially in the case of the Dalai Lama, amplified across multiple platforms, including organic adoption. While newsjacking may be used primarily for narrative amplification, the layered effect of combining it with other tactics can result in dramatic shifts in the information environment. Through hashtag hijacking and persona hijacking, influence actors operating en masse could dilute platform trust and push information consumers toward platforms they deem more trustworthy. Whoever controls the platform consumers turn to can dominate the narrative more easily than when competing with numerous actors across multiple platforms. Given the nature of building trust, the newsjacking platform must be easy to access but rooted in selective truths.

Conversely, the effectiveness of narrative and campaign hijacking was more challenging to assess. In the Fukushima case, it remains unclear whether the anti-nuclear sentiment was organically driven or state-amplified, and the PRC-attributed campaign hijacking targeting Taiwan's 2024 election failed to disrupt electoral outcomes, according to independent reporting. Only the H&M and the Dalai Lama campaign achieved widespread, real-world engagement. Persona hijacking suppressed dissent without high-volume public discourse. Activity attributed to PRC actors was most frequently observed on X, with additional spikes on Tumblr and Medium during narrative-centric operations.

5.3 Structural Strategies and Doctrinal Differences

Notably, the PRC does not appear to engage in traditional media hijacking through direct platform compromise. Instead, cyber attacks directed against Twitter/X and other platforms have been discovered to download account and user information that can later be used to target individuals offline or through coordinated inauthentic behavior online (Riley 2022). Deliberate media hijacking might instead use hacking to control the algorithms, data storage, or advertising feeds on those platforms (Vicens 2023). Media-adjacent activity (exemplified by the Paperwall network) illustrates a structural strategy distinct from direct platform compromise. Rather than hijacking existing media institutions, PRC-linked actors constructed parallel publishing ecosystems that simulate journalistic legitimacy while embedding pro-PRC narratives. This approach prioritizes long-term normalization of intimidation, content flooding, and other techniques over high-risk infrastructure takeover. In the case of native Chinese applications such as WeChat, frequent and deliberate censorship is the norm, and thus, media hijacking is unnecessary.

The communication hacking data obtained in our study indicates a philosophical difference between the Chinese Communist Party and the United States and Western nations. At the core, U.S. Psychological Operations forces focus on specific, measurable, and observable desired behaviors to ensure that evidence indicates the operation caused a behavior change (Department of the Army 2007). By prioritizing effectiveness measures, there is a high degree of accountability to the civilian military leadership. In contrast, the data indicate that the PRC actors prioritize performance measures and are more comfortable inferring correlations between activities and behaviors. The prioritization of performance measures explains the brute-force approach to persona-hijacking account creation and the widespread adoption of spamouflage. Without the requirement to account for activities to a democratic nation, PRC actors can pursue a variety of, often inappropriate, approaches. Occasionally, simple changes, such as a shift from "treated wastewater" to "toxic waste," do not necessarily constitute disinformation, even when they are misleading and deliberately applied. Instead, it represents an operationalization of "information for effect" as described in Army Doctrine Publication 3-13 (Department of the Army 2023). Furthermore, by prioritizing performance measures,

influence actors shorten the phases of information laundering and maximize the number of techniques and spreaders they can utilize (Harrell et al. 2025).

Overall, these cases indicate that communication hijacking operates along a spectrum of control, from individual-level suppression to ecosystem-level narrative embedding. This study represents a significant divergence from traditional information operations, in which activities are designed to persuade people to act. Instead, PRC-aligned influence actors demonstrate an aptitude for persuading inaction and diverting engagement from materials they deem to be against their objectives. The evolution of these tactics could easily result in a reversal of the participatory media ecosystem, in which user-generated content became ubiquitous and trusted. By deliberately proliferating obvious AI-generated content, lewd content, and inauthentic behavior, information actors push audiences back toward more centralized platforms where narratives are easier to control. The layers of communication hijacking indicate a transformation in which the desired behavior for the target audience is no longer to persuade belief in a narrative, but to deliberately increase ambiguity, distrust, and confusion.

5.4 Implications for Countermeasures

From Content Moderation to Layered Defense. Our findings suggest that PRC-linked influence activity is best understood as an effort to shape communicative sovereignty across digital arenas. Rather than focusing exclusively on false content, these operations intervene at multiple structural layers: controlling who speaks (persona), what is discoverable (hashtag), how events are interpreted (narrative), how institutions are perceived (campaign and brand), when attention peaks (newsjacking), and where legitimacy is anchored (media ecosystems). This layered perspective shifts analytical focus from content correction toward arena control. It highlights that state-linked influence operations may aim less at persuading audiences in isolated moments and more at gradually embedding preferred frames within contested informational environments. Recognizing these distinct layers suggests that countermeasures must be similarly differentiated. Defensive responses designed for one level of hijacking may not translate effectively to others.

A useful starting point is therefore the development of layer-specific defensive strategies aligned with the structural level targeted by an operation. Persona hijacking, for example, primarily exploits identity credibility and may require stronger identity verification systems, improved impersonation detection, and clearer provenance signals for influential accounts. Hashtag hijacking operates through discoverability manipulation and may require algorithmic controls capable of detecting coordinated flooding behavior or separating legitimate protest discourse from spam amplification. Narrative hijacking, by contrast, requires responses focused on framing and contextualization rather than simple fact-checking, as the objective of such campaigns is often to reframe existing events rather than fabricate new claims.

Temporal Dynamics and Strategic Communication. A second implication concerns the temporal dynamics of influence operations. Many campaigns leverage moments of heightened attention surrounding political crises, elections, or controversial policy announcements. Countermeasures may therefore benefit from early-warning mechanisms that detect emerging narrative injections before they reach peak visibility (Wu et al. 2025). Rapid-response communication strategies and pre-bunking efforts—where authoritative information is introduced before adversarial framing dominates—may help reduce the effectiveness of newsjacking and narrative manipulation during these high-attention windows.

The DISARM Blue Framework provides a promising taxonomy for countering influence operations; however, it currently lacks detailed operational guidance for deployment in contested environments. For instance, conceptual techniques such as "Hijack content and link to truth-based information" (technique C00032) require further procedural elaboration to be viable in high-volume, cross-platform environments.

The findings suggest that strategic communication may be as important as technical moderation (Argenti, Howell, and Beck 2005). Several campaigns—particularly those involving narrative hijacking and newsjacking—sought to reshape interpretive frames rather than propagate easily falsifiable claims. In such cases, debunking alone may be insufficient. Instead, countermeasures may involve proactive narrative framing, early contextualization of complex geopolitical events, and the amplification of credible sources before adversarial narratives become entrenched.

5.5 Research Agenda

Several avenues for further inquiry emerge. First, longitudinal analysis is needed to determine whether hijacking levels operate independently or interact dynamically over time. This includes assessing whether interventions targeted at specific hijacking levels influence adjacent levels and whether layered defensive strategies produce compounding protective effects. Second, clearer metrics are required to assess effectiveness beyond surface engagement indicators. This implies moving from manually selected case studies toward scalable, automated detection approaches capable of identifying hijacking operations across all levels in real time. Third, comparative analysis across state actors would clarify whether the differentiated model observed here reflects a uniquely PRC-linked strategy or broader patterns in contemporary influence operations. Comparative case studies—particularly across persona, narrative, and media-level interventions—may help identify where defensive efforts generate the greatest leverage within complex digital communication ecosystems. Finally, documenting successful countermeasures at specific hijacking levels will be essential to enable operational actors to deploy lessons learned across diverse communication environments in real time.

6 CONCLUSION

This study demonstrates that PRC-attributed influence activity cannot be reduced to isolated disinformation campaigns. Across seven cases, communication hijacking operated at multiple structural layers of the digital information environment—targeting individuals, discovery mechanisms, interpretive frames, institutional legitimacy, and media ecosystems. The variation observed across persona, hashtag, narrative, campaign, brand, newsjacking, and media-adjacent operations suggests adaptive, differentiated strategies rather than a single operational template.

By applying a layered communication hijacking framework, this research reframes influence activity as an effort to shape communicative sovereignty within contested digital arenas. The findings underscore that countering such activity requires more than content moderation; it demands level-specific interventions aligned with the structural target of control. As digital communication environments continue to fragment and hybridize, understanding how influence operations intervene across these layers will be essential for designing effective defensive strategies. Future work should test how disruptions at one level affect adjacent domains and whether layered defensive responses can mitigate structural arena manipulation in real time.

ABOUT THE AUTHORS

Dr. Donald Santacaterina is a currently a Threat Investigations Manager at 10a Labs, where he detects and mitigates national security and information operations abuse on GenAI platforms. He is an Open Source Intelligence Analyst, China Subject Matter Expert, and former Chinese Historian. He holds a Ph.D. in History (with a focus on Media Systems Propaganda) from UNC-Chapel Hill.

Maj. Daniel Eerhart is a research scientist at the Army Cyber Institute at West Point, specializing in psychological warfare. He earned his master's degree from the University of California, Los Angeles (UCLA) and has spent his career in the Army, primarily within the U.S. Army Special Operations Command (USASOC).

Lt. Col. Jason C. Brown is a research scientist and assistant professor at the Army Cyber Institute at West Point. He teaches risk management, organizational security, and systems-based decision making. As a futurist, he studies emerging threats, technological and social trends, and responses to those threats. He also leads a research team investigating critical infrastructure resilience on behalf of Army and other defense stakeholders. LTC Brown has worked within the intelligence, information operations, and cyber career fields. He has authored technical reports on the future of extremism, information warfare, cyber enabled financial crimes, microtargeting, and Chinese soft power. He holds a Ph.D. from Arizona State University.

Alex Nelson is a practitioner and researcher working at the intersection of national security, artificial intelligence, and operations in the information environment. His work focuses on applying open-source intelligence and data-driven analytical methods to identify, analyze, and counter state-sponsored information operations, disinformation, and other forms of strategic information manipulation. He holds an MA in International Relations and International Economics from The Johns Hopkins University, School of Advanced International Studies (SAIS) and a B.A. in International Security and Conflict Resolution from San Diego State University.

Dr. Brian Murphy is a senior manager in the private sector working at the intersection of cognitive security, national security, AI-enabled risk management, intelligence, and cybersecurity. He previously served as Acting Under Secretary for Intelligence and Analysis at the U.S. Department of Homeland Security, where he led intelligence, counterintelligence, security, cyber, and threat assessment activities for 250,000 personnel. Prior to DHS, Dr. Murphy served 20 years in the FBI, leading major cyber and counterintelligence operations, and

earlier was a U.S. Marine Corps officer. Dr. Murphy received his PhD from Georgetown University, an MA from Columbia University , and a BA from William and Mary. Dr. Murphy serves as an adjunct professor and published author at Georgetown University, focusing on intelligence, critical infrastructure, and threat mitigation. Dr. Murphy is the president of the Information Professionals Association.

ACKNOWLEDGMENTS

This project was made possible by a gratuitous vendor service agreement between Logically AI Inc. and the United States Military Academy. Three of the authors were affiliated with Logically at the time of this agreement. No authors received compensation beyond normal salaries for their work on this project.

REFERENCES

Angell, Rachel, Matthew Gorton, Paul Bottomley, Ben Marder, Sameer Bhaskar, and John White. 2020. "News You Can Use! Evaluating the Effectiveness of Newsjacking Based Content on Social Media." *Information Technology & People* 33 (2): 755–773. https://doi.org/10.1108/ITP-04-2019-0177.

Argenti, Paul A., Robert A. Howell, and Karen A. Beck. 2005. "The Strategic Communication Imperative." *MIT Sloan Management Review* (April 15, 2005). https://sloanreview.mit.edu/article/the-strategic-communication-imperative/.

Article 19. 2024. "In China, When Cyber Censorship Fails, Resort to Old-Fashioned Intimidation," March 12, 2024. https://www.article19.org/resources/blog-in-china-when-cyber-censorship-fails-resort-to-old-fashioned-intimidation/.

Associated Press. 2023. "Meta Closes Nearly 4,800 Fake Accounts in China That Tried to Polarize US Voters." The Guardian, November 30, 2023. https://www.theguardian.com/technology/2023/nov/30/china-fake-accounts-facebook-instagram.

Badham, Michael, and Vilma Luoma-aho. 2023. "Introduction to the Handbook on Digital Corporate Communication." In *Handbook on Digital Corporate Communication,* edited by Vilma Luoma-aho and Michael Badham, 1–16. Cheltenham, UK: Edward Elgar Publishing.

Badham, Michael, Vilma Luoma-aho, and Chiara Valentini. 2024. "A Revised Digital Media–Arena Framework Guiding Strategic Communication in Digital Environments." *Journal of Communication Management* 28 (2): 226–246. https://doi.org/10.1108/JCOM-03-2023-0031.

Bohman, Viking, and Hillevi Pårup. 2022. *Chinese Consumer Boycotts of Foreign Companies, 2008–2021.* July 11, 2022. https://kinacentrum.se/en/publications/chinese-consumer-boycotts-of-foreign-companies/.

Boyd, Andrew, and Dave O. Mitchell. 2016. *Beautiful Trouble: A Toolbox for Revolution.* New York: OR Books.

Brandt, Jessica. 2021. "How Autocrats Manipulate Online Information: Putin's and Xi's Playbooks." *The Washington Quarterly* 44 (3): 127–154. https://doi.org/10.1080/0163660X.2021.1970902.

Brumfiel, Geoff, Kat Lonsdorf, Rachel Carlson, Rebecca Ramirez, and Regina G. Barber. 2023. "We Unpacked Japan's Plan to Release Fukushima Wastewater." *NPR* (August 28, 2023). https://www.npr.org/2023/08/25/1195999316/we-unpacked-japans-plan-to-release-fukushima-wastewater.

Bundhun, Rebecca. 2023. "Fears Rise over Japan's Upcoming Release of Fukushima Nuclear Wastewater." *PBS News* (August 5, 2023). https://www.pbs.org/newshour/show/fears-rise-over-japans-upcoming-release-of-fukushima-nuclear-wastewater.

Burton, Nicholas, and Craig McClean. 2021. "Exploring Newsjacking as Social Media–Based Ambush Marketing." *Sport, Business and Management: An International Journal* 11 (2): 143–163. https://doi.org/10.1108/SBM-12-2019-0116.

Butler, Zak, and Jonas Taege. 2023. "Over 50,000 Instances of Dragonbridge Activity Disrupted in 2022." Google Threat Analysis Group, January 26, 2023. https://blog.google/threat-analysis-group/over-50000-instances-of-dragonbridge-activity-disrupted-in-2022/.

Cai, Derek. 2023. "Fukushima: China's Anger at Japan is Fuelled by Disinformation." *BBC News* (September 2, 2023). https://www.bbc.com/news/world-asia-66667291.

CCTV. 2021. ""抵制新疆棉花"？H&M失察！失策！失算！," March 4, 2021. http://m.news.cctv.com/2021/03/24/ARTIp0vSL8T4sKSDgRQcjlbS210324.shtml.

Cova, Bernard. 2022. "Ventolin: A Market Icon." *Consumption, Markets & Culture* 25 (2): 195–205. https://doi.org/10.1080/10253866.2021.2020761.

Datt, Angeli. 2021. "The CCP Hand Behind China's Xinjiang Cotton Backlash." *The Diplomat* (April 29, 2021). https://freedomhouse.org/article/ccp-hand-behind-chinas-xinjiang-cotton-backlash.

Davidson, Helen. 2023. "State-Backed Disinformation Fuelling Anger in China over Fukushima Water." *The Guardian* (September 4, 2023). https://www.theguardian.com/environment/2023/sep/04/state-backed-disinformation-fuelling-anger-in-china-over-fukushima-wastewater-japan.

Decode39. 2023. "Network of Fake, Pro-China "News" Websites Unveiled in Italy." Decode39, October 25, 2023. https://decode39.com/8109/network-fake-china-news-websites-italy/.

Department of the Army. 2007. *FM 3-05.301: Psychological Operations Process: Tactics, Techniques, and Procedures.* August 30, 2007. https://info.publicintelligence.net/USArmy-PsyOpsTactics.pdf.

Department of the Army. 2023. *ADP 3-13: Information.* Washington, DC: Headquarters, Department of the Army, November 27, 2023. https://irp.fas.org/doddir/army/adp3-13.pdf.

Doublethink Lab. 2024. "2024 Taiwan Elections. Influence Observation — Preliminary Statement," February 27, 2024. https://medium.com/doublethinklab/2024-taiwan-elections-foreign-influence-observation-preliminary-statement-caeeccb5b88e.

EEAS (European External Action Service). 2023. "Trade and Technology Council Fourth Ministerial – Annex on Foreign Information Manipulation and Interference in Third Countries," May 31, 2023. https://www.eeas.europa.eu/eeas/trade-and-technology-council-fourth-ministerial-%E2%80%93-annex-foreign-information-manipulation-and_en.

Eerhart, Daniel. 2024. "The Strategic Imperative: USASOC's Role in Advancing Civil Resistance Movements during Irregular Warfare." *Military Review* (November 1, 2024): 144–154. https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/Nov-Dec-2024/The-Strategic-Imperative/.

Ellis-Petersen, Hannah. 2023. "Dalai Lama Apologises after Kissing Boy and Asking Him to 'Suck My Tongue'." *The Guardian* (April 10, 2023). https://www.theguardian.com/world/2023/apr/10/dalai-lama-apologises-kissing-boy-suck-his-tongue-video.

EU DisinfoLab. n.d. "Doppelganger Hub." https://www.disinfo.eu/doppelganger-hub.

Feng, John. 2023. "What Full Video of Dalai Lama Kissing Boy Reveals." *Newsweek* (April 10, 2023). https://www.newsweek.com/dalai-lama-kisses-boy-tibet-video-1793401.

Fittarelli, Alberto. 2024. "PAPERWALL: Chinese Websites Posing as Local News Outlets Target Global Audiences with Pro-Beijing Content." The Citizen Lab, February 7, 2024. https://citizenlab.ca/research/paperwall-chinese-websites-posing-as-local-news-outlets-with-pro-beijing-content/.

Fruhwirth, L., and S. Nazari, eds. 2024. *Fool Me Once: Russian Influence Operation Doppelganger Continues on X and Facebook.* September 3, 2024. https://alliance4europe.eu/russian-influence-doppelganger-june-x-meta.

Gallagher, Ryan J., Andrew J. Reagan, Christopher M. Danforth, and Peter Sheridan Dodds. 2018. "Divergent Discourse Between Protests and Counter-Protests: #BlackLivesMatter and #AllLivesMatter." *PLOS ONE* 13 (4). https://doi.org/10.1371/journal.pone.0195644.

Gilbert, David. 2024. "ISIS Created Fake CNN and Al Jazeera Broadcasts." *Wired* (June 18, 2024). https://www.wired.com/story/isis-created-fake-cnn-and-al-jazeera-broadcasts/.

Graphika. 2023. *Deepfake It Till You Make It.* Graphika, February 7, 2023. https://graphika.com/reports/deepfake-it-till-you-make-it.

Harrell, Nicholas, Alexander Master, Nicolas Starck, and Daniel Eerhart. 2025. "Tactics and Techniques of Information Operations: Gaps in US Responses to Counter Malign Influence." In *Proceedings of the 20th International Conference on Cyber Warfare and Security (ICCWS 2025),* 122–132. https://doi.org/10.34190/iccws.20.1.3271.

Hautala, Miriam, Vilma Luoma-aho, and Jason C. Brown. 2025. "Communication Hijacked? New Vulnerabilities in the Digital Media Arenas." In *Handbook of Innovations in Strategic Communication,* edited by Shannon A. Bowen and Elina V. Erzikova, 358–370. Edward Elgar Publishing. https://doi.org/10.4337/9781035326488.00042.

Hautala, Miriam, Vilma Luoma-aho, and Jason C. Brown. 2026. "Communication hijacking: strategic communication gone dark." *Journal of Communication Management* 30 (1): 143–163. https://doi.org/10.1108/JCOM-09-2024-0171.

Hong, Yu. 2024. "Japan's Discharge of Nuclear-Contaminated Water Affects Its Exports." *CGTN* (March 11, 2024). https://news.cgtn.com/news/2024-03-11/Japan-s-discharge-of-nuclear-contaminated-water-affects-its-exports-1rSTZ4tZwGI/p.html.

Horwitz, Josh. 2019. "Amazon Faces Online Backlash in China for T-Shirts with Hong Kong Democracy Slogans." *Reuters* (August 15, 2019). https://www.reuters.com/article/world/amazon-faces-online-backlash-in-china-for-t-shirts-with-hong-kong-democracy-slog-idUSKCN1V50VZ/.

IAEA (International Atomic Energy Agency). 2023. "IAEA Finds Japan's Plans to Release Treated Water into the Sea at Fukushima Consistent with International Safety Standards," July 4, 2023. https://www.iaea.org/newscenter/pressreleases/iaea-finds-japans-plans-to-release-treated-water-into-the-sea-at-fukushima-consistent-with-international-safety-standards.

Joint Chiefs of Staff. 2022. *Joint Publication 3-04: Information in Joint Operations.* U.S. Department of Defense.

Kawashima, Shin. 2023. "Chinese Propaganda and Fukushima Treated Water Issue." *The Diplomat* (November 5, 2023). https://thediplomat.com/2023/11/chinese-propaganda-and-fukushima-treated-water-issue/.

Knüpfer, Curd, Matthias Hoffmann, and Vadim Voskresenskii. 2022. "Hijacking MeToo: Transnational Dynamics and Networked Frame Contestation on the Far Right in the Case of the '120 Decibels' Campaign." *Information, Communication & Society* 25 (7): 1010–1028. https://doi.org/10.1080/1369118X.2020.1822904.

Meerman, David Scott. 2015. "Newsjacking Your Way into the Media." In *The New Rules of Marketing and PR.* Wiley. https://doi.org/10.1002/9781119172499.ch22.

Milmo, Dan. 2024. "Iran-Backed Hackers Interrupt UAE TV Streaming Services with Deepfake News." *The Guardian* (February 8, 2024). https://www.theguardian.com/technology/2024/feb/08/iran-backed-hackers-interrupt-uae-tv-streaming-services-with-deepfake-news.

Ministry of Foreign Affairs of the People's Republic of China. 2023. "Foreign Ministry Spokesperson's Statement on the Japanese Government's Start of Releasing Fukushima Nuclear-Contaminated Water into the Ocean," August 24, 2023. https://www.mfa.gov.cn/eng/xw/fyrbt/fyrbt/202405/t20240530_11349809.html.

Murakami, Sakura. 2023. "Fukushima Wastewater Released into the Ocean, China Bans All Japanese Seafood." *Reuters* (August 24, 2023). https://www.reuters.com/world/asia-pacific/japan-set-release-fukushima-water-amid-criticism-seafood-import-bans-2023-08-23/.

Myers, Steven Lee, and Tiffany Hsu. 2024. "New Tactic in China's Information War: Harassing a Critic's Child in the U.S." *The New York Times* (June 27, 2024). https://www.nytimes.com/2024/06/27/business/china-disinformation-critics-harassment.html.

Nazari, S. 2024. "Collaborative Defense: Tackling Disinformation Against the EU Elections," June 6, 2024. https://alliance4europe.eu/first-summary-report-of-the-eu-election-network-pre-election-analysis.

Nimmo, Ben, C. Shawn Eib, and L. Tamora. 2019. *Cross-Platform Spam Network Targeted Hong Kong Protests: "Spamouflage Dragon" Used Hijacked and Fake Accounts to Amplify Video Content.* Graphika. https://public-assets.graphika.com/reports/graphika_report_spamouflage.pdf.

Noor, Dilshad. 2023. *In the Guise of Dalai Lama, China Targeted India and the Global Buddhist Summit.* DFRAC Digital Forensics, Research and Analytics Center, April 26, 2023. https://dfrac.org/en/2023/04/26/in-the-guise-of-dalai-lama-china-targeted-india-and-the-global-buddhist-summit-2/.

O'Sullivan, Stephen R. 2016. "The Branded Carnival: The Dark Magic of Consumer Excitement." *Journal of Marketing Management* 32 (9-10): 1033–1058. https://doi.org/10.1080/0267257X.2016.1161656.

O'Sullivan, Donie, Curt Devine, and Allison Gordon. 2023. "China Is Using the World's Largest Known Online Disinformation Operation to Harass Americans, a CNN Review Finds." CNN. https://www.cnn.com/2023/11/13/us/china-online-disinformation-invs.

Olson, Emily. 2023. "The Dalai Lama Apologizes for Asking a Young Boy to Suck His Tongue." *NPR* (April 10, 2023). https://www.npr.org/2023/04/10/1168962589/dalai-lama-apologizes-tongue-kiss.

Onstad, Katherine. 2024. *Performing Panda: Chinese Economic Coercion in the Era of Xi Jinping,* Kenney Paper 8. Air University Press, April 29, 2024. https://www.airuniversity.af.edu/AUPress/Display/Article/3757090/performing-panda-chinese-economic-coercion-in-the-era-of-xi-jinping/.

Pompili, Giulia. 2024. "Come Funziona la Rete di Fake News Cinesi." Il Foglio, February 8, 2024. https://www.ilfoglio.it/esteri/2024/02/08/news/come-funziona-la-rete-di-fake-news-cinesi-6194313/.

Reuters. 2023. *Dalai Lama Apologizes after Video Asking Boy to 'Suck My Tongue',* April 10, 2023. https://www.reuters.com/world/india/dalai-lama-apologises-after-video-asking-boy-suck-my-tongue-2023-04-10/.

Rich, Motoko, and John Liu. 2023. "China's Disinformation Fuels Anger Over Fukushima Water Release." *The New York Times* (August 31, 2023). https://www.nytimes.com/2023/08/31/world/asia/china-fukushima-water-protest.html.

Riley, Tonya. 2022. "Twitter Breach Exposes Anonymous Accounts to Nation State Hackers," August 5, 2022. https://cyberscoop.com/twitter-privacy-hacker-password-vulnerability/.

Sanderson, Jimmy, Katie Barnes, Christine Williamson, and Edward T. Kian. 2016. ""How Could Anyone Have Predicted That #AskJameis Would Go Horribly Wrong?"." *Public Relations Review* 42, no. 1 (March): 31–37. https://doi.org/10.1016/j.pubrev.2015.11.005.

Sarmiento, Prime. 2023. "Discharge Is against Right to Clean Environment, Activist Says." *China Daily* (August 25, 2023). https://global.chinadaily.com.cn/a/202308/25/WS64e7d9b7a31035260b81e196.html.

Satariano, Adam, and Paul Mozur. 2023. "The People Onscreen Are Fake. The Disinformation Is Real." The New York Times, February 7, 2023. https://www.nytimes.com/2023/02/07/technology/artificial-intelligence-training-deepfake.html.

Siano, Alfonso, Maria Giovanna Confetto, Agostino Vollero, and Claudia Covucci. 2021. "Redefining Brand Hijacking from a Non-Collaborative Brand Co-Creation Perspective." *Journal of Product & Brand Management* 31, no. 1 (March 1, 2021): 110–126. https://doi.org/10.1108/JPBM-03-2020-2780.

Siano, Alfonso, Agostino Vollero, and Alessandra Bertolini. 2022. "From Brand Control to Brand Co-Creation: An Integrated Framework of Brand Paradigms and Emerging Brand Perspectives." *Journal of Business Research* 152 (November): 372–386. https://doi.org/10.1016/j.jbusres.2022.08.001.

Steinfeld, Jemimah. 2023. "Critics of Beijing Face Increasing Impersonation Attacks." New Lines Magazine, August 21, 2023. https://newlinesmag.com/reportage/critics-of-beijing-face-increasing-impersonation-attacks/.

Suri, Manveena, and Rhea Mogul. 2023. "Dalai Lama Apologizes after Video Asking Child to 'Suck' His Tongue Sparks Outcry." *CNN* (April 11, 2023). https://edition.cnn.com/2023/04/10/india/dalai-lama-apology-kissing-boy-video-intl-hnk.

Terp, Simon, and Paul Breuer. 2022. "DISARM: A Framework for Analysis of Disinformation Campaigns." In *Proceedings of the IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA),* 1–8. IEEE. https://doi.org/10.1109/CogSIMA54611.2022.9830669.

The China Project. 2020. "Lululemon Faces China Boycott over 'Bat Fried Rice' Shirt," April 27, 2020. https://thechinaproject.com/2020/04/27/lululemon-faces-china-boycott-over-bat-fried-rice-shirt-2/.

Veil, Shari R., Jenna Reno, Rebecca Freihaut, and Jordan Oldham. 2015. "Online Activists vs. Kraft Foods: A Case of Social Media Hijacking." *Public Relations Review* 41, no. 1 (March): 103–108. https://doi.org/10.1016/j.pubrev.2014.11.017.

Vicens, A. J. 2023. "Twitter's Recommendation Algorithm Opens Platform to Manipulation, Bot Attacks, Researcher Finds," April 4, 2023. https://cyberscoop.com/twitter-algorithm-cve-bots-elon-musk/.

Warren, Patrick, Darren Linvill, Leland Fecher, Jayson Warren, Steven Sheffield, Jack Taylor, Alexa Gubanich, et al. 2023. *The 5-Year Spam: Tracking a Persistent Chinese Influence Operation.* Creative Inquiry Report. Clemson University Media Forensics Hub. https://open.clemson.edu/mfh_ci_reports/.

Weedon, Jen, William Nuland, and Alex Stamos. 2017. *Information Operations and Facebook.* Facebook Security. https://www.mm.dk/wp-content/uploads/2017/05/facebook-and-information-operations-v1.pdf.

Willis, Reilly A. Dempsey. 2020. "Habermasian Utopia or Sunstein's Echo Chamber? The "Dark Side" of Hashtag Hijacking and Feminist Activism." *Legal Studies* 40 (3): 507–526. https://doi.org/10.1017/lst.2020.16.

World Economic Forum. 2025. *Global Risks Report 2025.* World Economic Forum, February 15, 2025. https://www.weforum.org/publications/global-risks-report-2025/.

Wu, Z., Y. Liao, C. Luo, J. Shi, and Y. Yang. 2025. "Predicting Emerging Trends: A Machine Learning Approach to Topic Popularity on Social Media." *PeerJ Computer Science* 11:e3245. https://doi.org/10.7717/peerj-cs.3245.

Yamaguchi, Mari. 2023. "Fukushima Daiichi Nuclear Plant Starts 3rd Release of Treated Radioactive Wastewater into the Sea." *AP News* (November 2, 2023). https://apnews.com/article/japan-fukushima-water-release-efe6d5b02b29622707d0a220cdb78b20.

Zadrozny, Brandy. 2024. "Pro-Kremlin X Accounts Push Fake Fox News Articles Ahead of Debate." NBC News, June 27, 2024. https://www.nbcnews.com/tech/misinformation/-kremlin-x-accounts-push-fake-fox-news-articles-ahead-debate-rcna159301.

Zhang, Albert. 2024. "As Taiwan Voted, Beijing Spammed AI Avatars, Faked Paternity Tests and "Leaked" Documents." *The Strategist* (January 18, 2024). https://www.aspistrategist.org.au/as-taiwan-voted-beijing-spammed-ai-avatars-faked-paternity-tests-and-leaked-fake-documents/.

Zhang, Kaijun. 2024. "尚青》清德的私德." China Times. Opinion article, Shangqing Forum, January 11, 2024. https://www.chinatimes.com/opinion/20240111004171-262114?chdtv.

Received 31 March 2025; Revised 27 February 2026; Accepted 3 March 2026