A MACDONALD-LAURIER INSTITUTE PUBLICATION

TikTok: CHINA'S GLARING TROJAN HORSE

How Beijing uses the intensely addictive app for digital surveillance and influence operations

Sze-Fung Lee

May 2024

MLI
TRUE NORTH
IN CANADIAN PUBLIC POLICY

MACDONALD-LAURIER INSTITUTE

TRUE NORTH
IN CANADIAN PUBLIC POLICY

BOARD OF DIRECTORS

ADVISORY COUNCIL

RESEARCH ADVISORY BOARD

Contents

Executive summary | *sommaire* 4

Introduction 9

Methodologies 10

How does Beijing view TikTok? 11

- Xi Jinping's vision for big data
- TikTok's significance to Beijing

Threat I: Censorship, digital surveillance, and transnational repression 15

- Content censorship
- Data that TikTok has collected and its difference with Western Very Large Online Platforms (VLOPs)
- TikTok: Beijing's perfect surveillance tool
- TikTok's Data transfer to China: Chinese legal framework
- TikTok's Data transfer to China, the sneaky way: Backdoor and CapCut

Threat II: Foreign information manipulation and interference (FIMI) 21

- Chinese influence operations on TikTok: What's so special?
- Coercive measures
- Electoral interference
- Conspiracy theories
- Protecting China's image: Rebuke of "Western lies"
- TikTok's "For You" algorithm

Implications for Canada 30

Policy recommendations

- TikTok: Divest or face ban
- Laws and regulations for cross-border data transfer to foreign adversaries and data brokers
- Universal transparency practices with Very Large Online Platforms (VLOPs)
- Bolstering democratic resilience

Conclusion 37

About the author 38

References 39

Endnotes 48

Cover design: Renée Depocas (photo of hand holdling phone: Andrew Guan)

The author of this document has worked independently and is solely responsible for the views presented here. The opinions are not necessarily those of the Macdonald-Laurier Institute, its directors or supporters.

Executive summary | *sommaire*

Amidst the controversies over the “TikTok ban” is the struggle between free speech and concerns about Beijing’s malign use of the platform’s data to threaten national security and liberal democracies. Yet little research has delved into the question from Beijing’s perspective – how does the People’s Republic of China (PRC) view TikTok? What is the significance of the platform, and how does it differ from other Chinese and Western social media platforms such as Weibo, WeChat, Meta, and X in terms of digital surveillance and influence operations?

This paper aims to unfold how and why TikTok serves as Beijing’s strategic tool to advance its political narratives and strategic agendas and the unique features of TikTok that enable it to fulfil that purpose. It explores how the PRC influence operations (IOs) are integrated with cognitive warfare tactics to manipulate the information environment on TikTok to coerce, sow confusion, magnify division, and conduct electoral interference in liberal democracies. Finally, the paper proposes policy recommendations to mitigate the threats posed by TikTok.

The first section focuses on Chinese leader Xi Jinping’s ambition for big data: how Beijing views and leverages TikTok for influence operations, and how data harvesting and mass surveillance fits into its grand strategy. It discusses TikTok’s speciality – producing and sharing short, influential, and addictive video content with billions of international users – and how this content facilitates biometric data harvesting and amplifies the effectiveness of Beijing’s digital surveillance and influence operations, bolstering the PRC’s goals in ways that other Chinese and Western social media platforms cannot. Closely tied to the Cyberspace Administration of China (CAC) – the PRC’s national internet regulator and censor – TikTok is a one-of-a-kind app that has become a Trojan Horse used by the PRC to gain invaluable access to and influence over Western democracies.

The second section concentrates on the data privacy issue: how data TikTok has collected differs from other Western “Very Large Online Platforms” (VLOPs), and how the PRC utilizes it for digital surveillance and transnational repression via initiatives such as “Project Raven,” which saw TikTok used to spy on Western journalists after they reported

on the app's repeated access of US user data. This section also discusses how TikTok's data could be transferred to the PRC under China's legal framework and through other unorthodox means such as backdoor codes and its in-app-linked video template software CapCut. Additionally, TikTok's extensive global reach and pervasive data collection infrastructure imply that most of the PRC's targets – journalists, activists, researchers, and China critics – could be subjected to Beijing's mass surveillance, regardless of their geographic location and even if they are not using TikTok.

The third section investigates how Beijing leverages TikTok as a strategic tool to manipulate the information ecosystem while integrating cognitive warfare tactics that exploit vulnerabilities in human psychology for influence operations. Various case studies will be included to illustrate how the PRC and its affiliated entities utilize TikTok's characteristics to maximize the impact of their influence operations. Recent IOs that amplified Beijing's political narratives and strategic agendas include:

- disinformation campaigns during Taiwan's presidential and legislative election;
- grey-zone activities around the Kinmen islands, located just off mainland China but controlled by Taiwan;
- conspiracy theories claiming that the US created the COVID-19 virus;
- and rebukes of "Western lies" about the PRC's use of forced labour and the oppression of certain ethnic minorities within China, especially in the Xinjiang Uyghur Autonomous Region (XUAR).

I also explore the tactics, techniques, and procedures (TTPs) during IO events, as well their connection to the PRC and/or PRC-affiliated entities.

The paper will show how TikTok's "For You" algorithm partially shares server codes with another of ByteDance's apps, Douyin (the Chinese version of TikTok) – and explain how these algorithm codes are likely subjected to the PRC's regulations on internet censorship and recommendation algorithms – manipulating what videos are visible and amplified for users.

The fourth section reveals some of the TikTok IOs that have targeted Canadians and discusses the implications for Canada if it fails to urgently act to protect the personal data of its citizens.

The final section proposes policy recommendations to mitigate the threat posed by TikTok and other China-based social media. For the US, this includes executing the recently passed *Protecting Americans from Foreign Adversary Controlled Applications Act*. In Canada, I argue for the enforcement of ByteDance's divestiture from TikTok under the *Investment Canada Act*.

Given TikTok's vast reach and influence, a key goal should be to compel it to divest from its Beijing-based parent company. Doing so would greatly help to protect our sensitive data from the PRC – especially since there are no other PRC-linked apps waiting in the wings to fill the gap of TikTok's significance. Other longer-term solutions include:

- banning cross-border data transfer to foreign adversaries;
- scrutinizing laws and regulations for data brokers;
- mandating VLOPs to investigate and report on influence operations as universal transparency practices;
- and engaging in education campaigns and strategic communications initiatives that bolster democratic resilience.

It is imperative for like-minded democracies to take more rigorous measures to mitigate the risk posed by TikTok and ByteDance as soon as possible. MLI

***Au cœur des polémiques** entourant l'interdiction de TikTok se trouve la bataille entre la liberté d'expression et l'intérêt pressenti de Beijing d'en faire un usage pernicieux contre la sécurité nationale et les démocraties libérales. Pourtant, peu d'études se sont penchées sur la position de Beijing – comment la République populaire de Chine (RPC) entrevoit-elle TikTok? Quelle est l'importance de la plateforme et en quoi diffère-t-elle des autres médias sociaux chinois ou occidentaux comme Weibo, WeChat, Meta et X sur le plan de la surveillance numérique et des activités d'influence (AI)?*

Ce document vise à décrire comment et pourquoi TikTok sert d'outil tactique pour promouvoir les discours politiques et les stratégies de Beijing, ainsi que les attributs uniques de TikTok pour atteindre cet objectif. Il explore comment les AI de la RPC sont intégrées aux tactiques de « guerre cognitive » en vue de manipuler l'information sur TikTok pour contraindre, semer la confusion, amplifier les divisions et s'ingérer dans les processus électoraux et les démocraties libérales. Enfin, dans ce document, on propose des recommandations stratégiques pour atténuer le risque posé par TikTok.

La première partie s'intéresse aux aspirations du dirigeant chinois Xi Jinping à l'égard des mégadonnées : la vision et le rôle de TikTok pour Beijing en matière d'AI et la place de la collecte de données et de la surveillance de masse dans sa grande stratégie. Elle décrit les particularités de TikTok – production et partage de contenus vidéo courts, influents et addictifs pour des milliards d'utilisateurs internationaux – et de quelle manière ces contenus peuvent faciliter la collecte biométrique et renforcer la surveillance numérique et les AI de Beijing, tout en soutenant les objectifs de la RPC comme aucune autre plateforme, occidentale ou chinoise. Étroitement liée à la Cyberspace Administration of China *(organisme national de régulation et de censure de l'internet), TikTok est une appli unique en son genre devenue un « cheval de Troie » pour la RPC, qui l'utilise pour un accès irremplaçable aux démocraties occidentales et l'exercice d'influence.*

La deuxième partie porte sur la confidentialité des données : comment les données recueillies sur TikTok diffèrent de celles d'autres très larges plateformes en ligne (VLOP) occidentales et sont utilisées par la RPC à des fins de surveillance numérique et de répression internationale par l'intermédiaire d'initiatives comme le « projet RAVEN »

– à l'issue duquel TikTok a servi à des activités de surveillance auprès de journalistes occidentaux qui avaient révélé les fréquents accès de l'appli à des données utilisateur américaines. Cette partie aborde également le transfert des données de TikTok vers la RPC, rendu possible par le cadre juridique chinois et d'autres moyens d'intermédiation peu orthodoxes comme les « portes dissimulées » et CapCut, la plateforme de montage vidéo intégrée. Par ailleurs, la portée mondiale de TikTok et sa puissante infrastructure de collecte signifient que la plupart des cibles de la RPC – journalistes, militants, chercheurs et détracteurs – peuvent faire l'objet d'une surveillance de masse, peu importe leur situation géographique ou s'ils utilisent ou non TikTok.

La troisième partie analyse comment Beijing fait de TikTok un instrument de manipulation dans l'écosystème d'information, tout en intégrant, dans le cadre des AI, des tactiques de « guerre cognitive » exploitant la fragilité psychologique humaine. Diverses études de cas illustrent comment la RPC et ses entités affiliées utilisent TikTok pour maximiser l'impact de leurs AI. Parmi les plus récentes qui ont amplifié les discours politiques et les agendas stratégiques de Beijing, on retrouve :

- *les campagnes de désinformation à l'approche des élections présidentielles et législatives à Taïwan;*
- *les activités « zone grise » autour des îles Kinmen, à proximité de la Chine continentale, mais contrôlées par Taïwan;*
- *les théories complotistes affirmant que les États-Unis ont développé le virus COVID-19;*
- *les désaveux des prétendus mensonges occidentaux sur le travail forcé et l'oppression de certaines minorités ethniques en Chine, surtout dans la Région autonome ouïgoure du Xinjiang (RAOX).*

J'explore également les tactiques, techniques et procédures associées aux AI et leurs liens avec la RPC et ses entités affiliées.

- *Ce document montre comment l'algorithme « Pour toi » de TikTok partage certains codes serveur avec une autre appli de ByteDance, Douyin (la version chinoise de TikTok) – et explique comment ces codes sont vraisemblablement assujettis aux réglementations de la RPC sur la censure de l'internet et le système de recommandations – de manière à contrôler quelles vidéos seront visibles ou « amplifiées » pour les utilisateurs.*
- *La quatrième partie présente certaines AI de TikTok qui ont ciblé des Canadiens et les conséquences pour le Canada s'il n'agit pas de toute urgence pour protéger les données personnelles des citoyens.*

*La dernière partie propose des recommandations stratégiques contre le risque posé par TikTok et d'autres médias sociaux basés en Chine. Pour les États-Unis, il s'agit de faire appliquer la loi récemment adoptée qui prévoit l'interdiction de TikTok (*Protecting Americans from Foreign Adversary Controlled Applications Act*). Au Canada, l'entreprise ByteDance doit être dessaisie de TikTok en vertu de la* Loi sur Investissement Canada.

Compte tenu de la portée et de l’influence de TikTok, le principal objectif doit être de la contraindre à se désengager de sa société mère basée à Beijing. Cela contribuerait grandement à protéger nos données de nature délicate, d’autant plus qu’aucune autre appli liée à la RPC n’attend dans les coulisses pour remplacer l’immense espace comblé par TikTok. D’autres solutions à plus long terme existent, notamment les suivantes :

- *le bannissement des transferts transfrontaliers de données à des adversaires étrangers;*
- *l’examen minutieux des législations et réglementations relatives aux courtiers en données;*
- *l’obligation pour les VLOP d’enquêter et de faire rapport sur les AI, conformément aux pratiques reconnues en matière de transparence;*
- *la participation à des campagnes de sensibilisation et de communication stratégique renforçant la résilience démocratique.*

Il est impératif que les démocraties aux vues similaires prennent rapidement des mesures rigoureuses pour mitiger le risque posé par TikTok et ByteDance. MLI

Introduction

On April 23, 2024, the US Senate passed a bill that would force TikTok's parent company, Beijing-based ByteDance, to either divest from TikTok or face a ban in the United States (Maheshwari and McCabe 2024a). While the bill received broad bipartisan support and President Joe Biden signed it into law the next day, it remains controversial, with critics warning about its impact on free speech, fair competition and/or market dominance in the social media landscape, the effectiveness of the bill, and more.

However, at the heart of this approach is the rising awareness of Beijing's malign use of the platform's data to threaten national security and undermine our democratic system. The "TikTok ban" can be seen as a (likely) short-term victory by Washington over the PRC's creeping influence on the digital front. It also sets a precedent for other liberal democracies, showing how they, too, can combat Beijing's hostile influence operations, electoral interference, and mass surveillance.

Thanks to the debates over the "TikTok ban," there is a growing awareness worldwide about the PRC's leveraging of the app for both data exploitation and sowing division in targeted countries. However, it raises the question – how does Beijing itself see TikTok? How significant is the app to the PRC's geopolitical strategy? How do TikTok's unique characteristics enable the PRC and PRC-affiliated entities to proliferate digital influence operations and data harvesting? And, how is TikTok different from other Chinese and Western social media platforms such as Weibo, WeChat, Meta, and X?

This paper aims to shed some light on these answers via analysis of Beijing's hybrid warfare strategies, data-driven governance, internet censorship and regulations, and legislation and policies. In addition, concrete case studies will reveal clear instances of influence operations involving TikTok – illustrating how Beijing and its affiliated entities integrated cognitive warfare tactics with TikTok's characteristics to steer public discourse on matters it deems vital to its interest.

Methodologies

This report leverages Open-Source Intelligence Techniques (OSINT) to examine publicly available data from websites and social media platforms. It utilizes several types of qualitative information. It relies primarily on indigenous sources, such as the PRC government's official documents, legislation, press releases, statements, and speeches by officials including Xi Jinping and spokespersons of China's Ministry of Foreign Affairs – and accompanied by Chinese state-affiliated media reports and research publications – to gain a comprehensive understanding of TikTok's affiliation with the PRC and PRC-affiliated entities, as well as its significance to Beijing.

In addition to TikTok/ByteDance's official privacy policies, a variety of secondary sources including Western media's investigation of TikTok – for instance, TikTok's surveillance on BuzzFeed/*Forbes* journalists – as well as previous studies from prominent think tanks on the platform's data exploitation, surveillance, and censorship system are also used as references for the report.

For the case studies of the PRC/PRC-affiliated influence operations on TikTok, a combination of social media monitoring and off-the-shelf tools were used to collect publicly available data. The timeframe for collecting the data from TikTok was January 1, 2022 to March 31, 2024, which allows the capture of the most relevant case studies of the PRC and PRC-affiliated entities' influence operations on the platform in the past three years. A diverse set of neutral keywords and phrases in English, Mandarin Chinese, and Cantonese languages, was employed to surface relevant content. I then examined the collected data to identify patterns, trends, and attributions of the influence operations for analysis.

How does Beijing view TikTok?

Xi Jinping's vision for big data

Chinese leader Xi Jinping's ambition to leverage big data to fuel China's socio-economic development and tighten national security has long been the PRC's key strategy since his presidency. In 2013, Xi noted that data is like the new "oil resources," it is transforming states' comprehensive national power, and "whoever controls big data will have the upper hand" (China News Service 2015). Xi views data as strategic and economic assets, and along with data infrastructure, is vital for national development and security. Therefore, controlling and utilizing data is a crucial part of the PRC's grand strategy.

Throughout the years, Beijing has implemented various policies and tactics – both legal and illegal – to control data it deems necessary for China's "security" and development. Launched in October 2023, the National Data Bureau (NDB) (国家数据局) – a new institution established by the State Council, managed by the National Development and Reform Commission (NDRC) that aims at integrating data resources across the country and beyond for its utilization – is a manifestation of Xi's ambition for big data (The Paper 2023).

Given China's immense geography and large population, the PRC relies heavily on data and technology to govern. "E-governance" and smart cities, for instance, integrate critical infrastructure with surveillance technologies like smart lampposts that include Bluetooth beacons, Radio Frequency Identification (RFID) tags to collect real-time data (Gleeson 2019), and 360-degree panoramic cameras with hardware connected to the Chinese "Skynet" facial recognition surveillance network (Takeshi 2019). These strategies enable the PRC to control the flow of digital information and ultimately, Chinese citizens both at home and abroad, while also influencing overseas audiences – all in the name of "national security."

TikTok's significance to Beijing

Chinese social media platforms play a key role in executing and supporting the PRC's data-driven governance – specifically in the areas of digital surveillance, transnational repression, and IOs – and TikTok serves as Beijing's perfect strategic tool to advance these political narratives and strategic agendas.

Stating the obvious, TikTok's parent company – Beijing ByteDance Technology Co. Ltd. – is a Chinese company based in Beijing. The Cyberspace Administration of China (CAC) (国家互联网信息办公室) – is managed by the Office of the Central Cyberspace Affairs Commission (中央网络安全和信息化委员会) (The People's Republic of China 2022), which is headed by Xi Jinping (Xinhua 2023) – has a stake and a board seat in ByteDance. In 2021, CAC took a 1 percent stake in ByteDance through WangTouZhongWen (Beijing) Technology, a company owned by the China Internet Investment (Yang and Goh 2021). The latter was established by the CAC and the Ministry of Finance in 2017 (China Central Television 2017)

In essence, the CAC's main job is to regulate China's internet system and execute propaganda online, especially targeting negative public opinion worldwide (Zhang, Hoja, and Latimore 2023). Hence, its move to exert control on the social media platform showcases TikTok's strategic worthiness. This is linked to how IOs are being amplified on TikTok in alignment with the CAC's responsibilities, which will be discussed in detail in "Protecting Chinas' image: Rebuke of 'Western lies,'" page 24.

While the CAC remains a key actor, ByteDance's ties with PRC state entities are not limited to a single government body. For instance, ByteDance had a strategic cooperation agreement with the PRC's Ministry of Public Security (MPS) for Douyin (the Chinese version of TikTok) to engage in "in-depth cooperation" with its News and Publicity Bureau (公安部新闻宣传局) in new media content creation and production to "tell the police officers' story well" (讲好警察故事) – aiming to further enhance MPS's credibility, influence, and outreach capability (*People's Daily* 2019). In 2018, a total of 170 provincial and prefectural-level public security organs created their Douyin accounts and jointly established a "One-Click Reporting by Cyber Police" mechanism in the platform. This system allows posts' content to be promptly prioritized in the system's specialized review queue for "appropriate actions" once they are reported by the cyber police officers (*Southern Metropolis Daily* 2018).

In addition, the PRC has announced several regulations on internet censorship and recommendation algorithms such as the "Provisions on the Governance of the Online Information Content Ecosystem" (网络信息内容生态治理规定) and the "Provisions on the Management of Algorithm Recommendations in Internet Information Services" (互联网信息服务算法推荐管理规定) in the past five years [details in "TikTok's 'For You' algorithm," page 28]. These regulations often emphasize promoting "positive energy" while cracking down on content that "threatens national security" or "disrupts socio-economic stability." And Beijing's tightening control over the information space is accompanied by its ambition to leverage AI-governance both at home and abroad. TikTok's "For You" algorithm, which mirrors Douyin's algorithm as they partially share server codes, thus serves as the perfect tool for Beijing to pump its political narratives on the platform.

The unique characteristics of TikTok enable it to serve as Beijing's best strategic tool – more so than any other Chinese social media.

The unique characteristics of TikTok enable it to serve as Beijing's best strategic tool – more so than any other Chinese social media. With more than a billion active users, TikTok's key feature – short reels – has inspired the creation of countless user videos. When TikTok was first launched, it leveraged idols and influencers to promote dancing videos and/or lip-syncing clips which encouraged users to record themselves dancing with the featured songs – hence the trending hashtags #TikTokdancechallenge and #lipsyncchallenge. As these videos mainly focus on the users' faces, voices, and body movements, TikTok is able to harvest biometric identifiers and biometric information such as faceprints and voiceprints far more efficiently than other social media platforms like Weibo or Meta.

TikTok's privacy policy also states that the company collects information about the videos, images, and audio of one's user content, such as "identifying the objects and scenery that appear, the existence and location within an image of face and body features and attributes, the nature of the audio, and the text of the words spoken" (TikTok 2023).

As the PRC's surveillance system struggles with facial recognition across different ethnicities, the billions of TikTok videos supply crucial data from international users that helps to fill the gap. The diversity of data – various races in multiple accents and language settings – could be used to train PRC's mass surveillance algorithm and enhance its technologies to a more efficient and far-reaching capability.

Secondly, visual-based disinformation is more effective in attracting attention and garnering engagement. The volume of information Beijing pumps into TikTok during a large-scale IO leverages cognitive warfare tactics to overwhelm human attention span via saturation of information space, thus constituting a more favourable condition for sowing confusion and influencing public opinion on a certain topic (Hung and Hung 2022). This will be discussed in detail in section 6.

In addition to being a video-based platform, the other key difference between TikTok and other Chinese social media apps is that it has gained billions of users overseas.

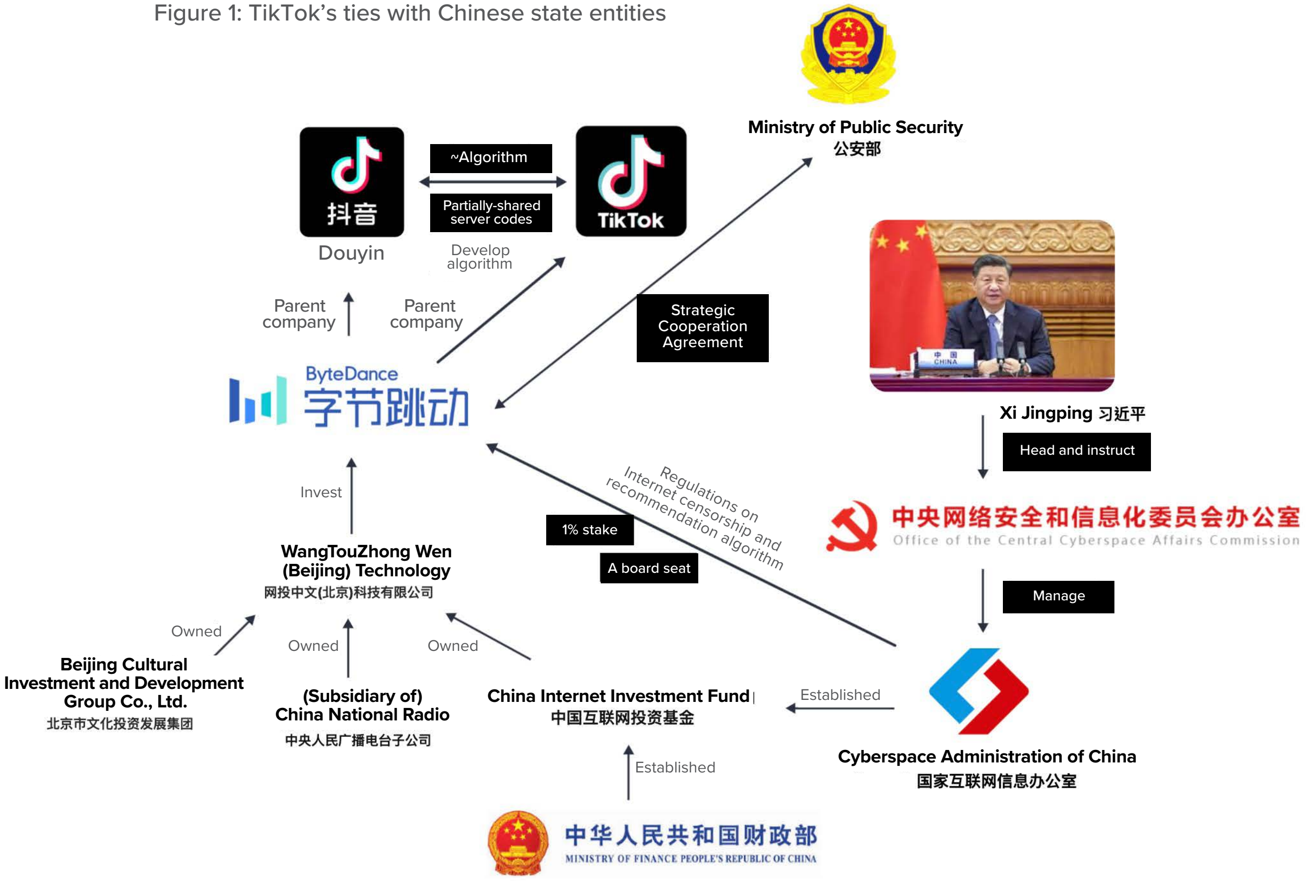
Despite Chinese platforms like Weixin/WeChat, Weibo, and Xiaohongshu having millions of users, especially when it comes to the diaspora communities, they are mainly rooted in the Chinese language, and thus not easily accessible or popular among non-Chinese language speakers. Although these platforms are highly infiltrated by Beijing's political propaganda and influence operations, they have limited reach in terms of attracting a general audience in foreign countries.

On the other hand, TikTok is compiled in multiple languages and has over 1 billion active users worldwide, with 170 million users in the US (*The New York Times* 2024). Given Canada's proximity to the US, Canadian TikTok content creators and users are also heavily "plugged-in" to the American TikTok market (Fowler 2024).

TikTok's outreaching capability and potential for IOs makes it also a uniquely powerful tool for political mobilization. This was recently demonstrated during TikTok's attempts to leverage the social media platform to urge Americans to call their representatives in Congress to voice opposition to the proposed (now passed and signed) "TikTok ban" (Kern and Bordelon 2024).

Thus, TikTok constitutes a valuable strategic asset for Beijing. It is not only a one-of-a-kind app that cannot be easily replicated by other Chinese social media – but it is also the first Trojan Horse app that was able to gain entry to the Western camp. Figure 1 illustrates TikTok's ties with Chinese state entities.

Figure 1: TikTok's ties with Chinese state entities


Ministry of Public Security
公安部
抖音
Douyin
~Algorithm
Partially-shared server codes
TikTok
Develop algorithm
Parent company
Parent company
Strategic Cooperation Agreement
ByteDance
字节跳动
Xi Jingping 习近平
Head and instruct
中央网络安全和信息化委员会办公室
Office of the Central Cyberspace Affairs Commission
Manage
Invest
Regulations on Internet censorship and recommendation algorithm
1% stake
A board seat
WangTouZhong Wen (Beijing) Technology
网投中文(北京)科技有限公司
Owned
Owned
Owned
Beijing Cultural Investment and Development Group Co., Ltd.
北京市文化投资发展集团
(Subsidiary of) China National Radio
中央人民广播电台子公司
China Internet Investment Fund
中国互联网投资基金
Established
Cyberspace Administration of China
国家互联网信息办公室
Established
中华人民共和国财政部
MINISTRY OF FINANCE PEOPLE'S REPUBLIC OF CHINA

Source: Created by author

Threat I: Censorship, digital surveillance, and transnational repression

Content censorship

Previous studies have indicated that TikTok manipulated its information system for certain topics that are considered politically sensitive to the PRC. A report from the Network Contagion Research Institute at Rutgers University last year showed that topics often suppressed by the PRC in the Chinese information space like Hong Kong protests (Nimmo, Eib, and Tamora 2019) and the oppression of China's Uyghur population "appear to be unusually underrepresented on TikTok" compared with Instagram (Maheshwari 2023).

Research conducted by the Australia Strategic Policy Institute (ASPI) also found that TikTok suppressed #LGBTQ+ related issues in the form of hashtags in at least 8 languages – the platform falsifies the impression that these posts are searchable, when in fact they are being categorized like swear words or terrorism content in TikTok's code (Ryan, Fritz, and Impiombato 2020). Another prominent example would be #Xinjiang-related issues. Instead of surfacing topics like Xinjiang's forced labour or "re-education" camps, TikTok appears to pump PRC propaganda aimed at "Telling China's Story Well" (讲好中国故事) (Xinhua 2013) and rebuking Western "political lies" (China's Ministry of Foreign Affairs 2024). The abundant number of videos for the latter is likely due to the role of the CAC, which will be discussed in "Protecting China's image: Rebuke of 'Western lies,'" page 24.

TikTok's Privacy Policy states that "when you create User Content, we may upload or import it to the Platform before you save or post the User Content (also known as pre-uploading)" (TikTok 2023). Pre-uploading implies that the content is being reviewed by TikTok before it becomes publicly available – in other words, censorship could and is likely to occur at this stage. In the case of the censorship system in Weixin/WeChat, the Chinese platform filters a blacklist of keywords (Knockel et al. 2020) and images (Ruan, Knockel, and Crete-Nishihata 2020) that are considered politically sensitive to the regime. Even though China's censorship system remains opaque, it likely involves pre-upload filtering of text and images.

TikTok's definition of information collected for "content moderation" and recommendations, and "other non-personally identifying operations" is merely a matter of framing. The content that TikTok users view has likely undergone a certain level of surveillance and censorship.

Data that TikTok has collected and its difference with Western Very Large Online Platforms (VLOPs)

Apart from what is normally collected from Western VLOPs – IP address, geolocation-related data, cookies, browsing and search history, as well as other metadata – TikTok acquired Media Access Control (MAC) addresses, which are 12-digit unique device identifiers in electronics, and collected the information for at least 15 months (Poulsen and McMillan 2020). As MAC addresses cannot be reset or altered, they thus enable the gathering of intel over lengthy periods of time – regardless of any other operation security measures implemented – unless one gets a new device. In other words, even if you uninstall TikTok and reset your phone to factory settings, your MAC address, which can identify you, is still the same.

While both the Apple Store and Google Play Store banned third-party apps from obtaining MAC addresses, TikTok bypassed that restriction by "using a workaround that allows apps to get MAC addresses through a more circuitous route," according to a *Wall Street Journal* investigation. When TikTok is first installed in a device, it secretly captures the MAC address and sends it to ByteDance, allowing the company to conduct "ID bridging" – a tactic of "connecting the old advertising ID to a new one" (Poulsen and McMillan 2020).

Moreover, TikTok also stores location information based on your SIM card, which is not normally harvested by other big tech due to privacy concerns (SIM card data, which contains your phone number or mobile network/carrier, also enables precise location tracking).

While TikTok stated that the current version "does not collect precise or approximate GPS information from US users," it also noted, "if you are still using an older version that allowed for collection of precise or approximate GPS information (last release in August 2020) and you granted us permission to do so, we may collect such information" (TikTok 2023). It appears that TikTok, in some way, admits that it had acquired users' precise locations before August 2020, and will continue to have that data unless they opt out.

TikTok: Beijing's perfect surveillance tool

Over the years, TikTok has faced repeated allegations of conducting surveillance on individuals. In 2022, TikTok/ByteDance launched the covert operation "Project Raven" to spy on multiple journalists who covered the story that revealed the company's ties with the PRC. According to *Forbes*, "Project Raven" involved TikTok's Head of Global Legal Compliance (Chief Security and Privacy Office) and was overseen in ByteDance's Internal Audit and Risk Control department, which is led by its executive Song Ye, who reports to ByteDance co-founder and CEO Rubo Liang, who are all based in China (Baker-White 2022a). The operation tracked three journalists – Emily Baker-White, Katharine Schwab, and Richard Nieva – via improper access to their IP addresses and other relevant user data – in an attempt to identify TikTok/ByteDance's whistle-blower. (Baker-White 2022b).

In the eyes of Beijing, TikTok is likely the perfect tool for digital surveillance and transnational repression. While security-conscious journalists, activists, and researchers may have taken measures to protect their data from TikTok/ByteDance, their family, friends, and colleagues may not – and that could thwart their mitigation strategies and expose them to severe risks, even if they themselves are not using TikTok.

When a TikTok user signs up or logs in to the platform using a third-party service such as Facebook, Instagram, X (formerly Twitter), or Google, or links their account to a third-party service, TikTok could collect data from that service, including the user's email and contact list. Given the fact that TikTok has over a billion users around the globe, this implies that most of the PRC's targets – for instance, the twelve primary targets of the United Front Work Department (UFWD), which is a Chinese government agency that reports directly to the CCP's Central Committee and is designed for operations targeting Chinese communities abroad – are likely under Beijing's mass surveillance microscope. These included ethnic and regional minorities such as the Uyghurs and Tibetans, as well as Taiwanese, residents of Hong Kong and Macau, as well as overseas Chinese diaspora communities (Charon and Jeangène Vilmer 2021), especially those who participated or advocated for pro-democracy and human rights.

TikTok's data transfer to China: Chinese legal framework

Multiple pieces of legislation have been brought into force in the past decade to support Xi Jinping's ambition to leverage data for the PRC's agendas, including: the *State Security Law* (2015), the *Cybersecurity Law* (enacted in 2016, it went into effect in 2017), the *Intelligence Law* (2017), *Measures on Cybersecurity Review* (2020), and the *Data Security Law* (2021); an entire legal framework is built to force Chinese companies to hand over their data (*China Daily* 2015).

The *Chinese Cybersecurity Law* (Chapter 3, Section 1, Article 28), for instance, states that "network operators shall provide technical support and assistance to the public security entities and national security entities for maintaining national security and investigating criminal activities" (Cyberspace Administration of China 2016). Given that ByteDance is a Chinese company based in Beijing, it has the legal responsibility to "provide assistance" including giving up its subsidiary (TikTok)'s data to the PRC (He 2024).

Despite TikTok's CEO Chew Shou-Zi having repeatedly claimed that the company has "never shared, or received a request to share, US user data with the Chinese government" and "nor would TikTok honour such a request if one were ever made" (Shepardson 2023), the reality remains crystal clear – under *Chinese Intelligence Law* (Article 7), all organizations (including ByteDance) are compelled to "support, assist, and cooperate with the national intelligence work" and "keep secrets of the national intelligence work that they knew" (National People's Congress 2017). This implies that ByteDance could have turned over foreign users' data, in accordance with Chinese law, and is obliged to keep that secret from the public.

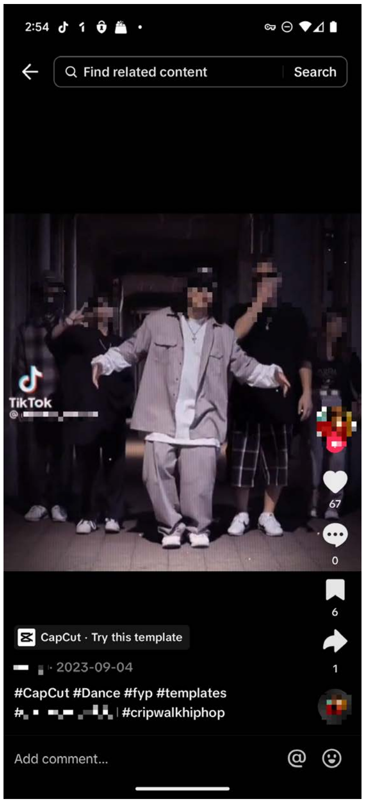
TikTok's data transfer to China, the sneaky way: Backdoor and CapCut

As previous studies – including an investigation of more than 80 hours of leaked audio recordings of internal TikTok meetings – have indicated, TikTok's user data has been repeatedly accessed from China, and some US users' data is stored in China (Baker-White 2022 Levine 2023). A lawsuit filed against ByteDance last year alleged that the company built a "backdoor channel in the code," which would allow "certain high-level persons to access user data, no matter where the data is located, even if hosted by a US company with servers located in the US" (Whateley and Rodriguez 2023).

While it is common knowledge that data collected by TikTok could be transferred to China given its company infrastructure, there is also a more direct way that foreign users would give up their data to Beijing "voluntarily." As mentioned above, the #TikTokdancechallenge is one of the most popular videos created on the platform. And a lot of those dancing challenge clips come along with a video template – a pre-designed framework with some customizable features for users to create a similar video on their own. This video template service is provided by CapCut – and all of its mobile application, desktop, and website services are provided and controlled by ByteDance.

When a user clicks on the "use template in CapCut", the interface pops up a modal written "Terms of Service and Privacy Policy," which requires a click on the "Agree and continue" to use the feature. By tapping the "Agree and continue" button, the user "agree(s) to CapCut's Terms of Service and acknowledge that you have read our Privacy Policy and Cookies Policy to learn how we collect,

FIGURE 2A: TikTok video with CapCut feature

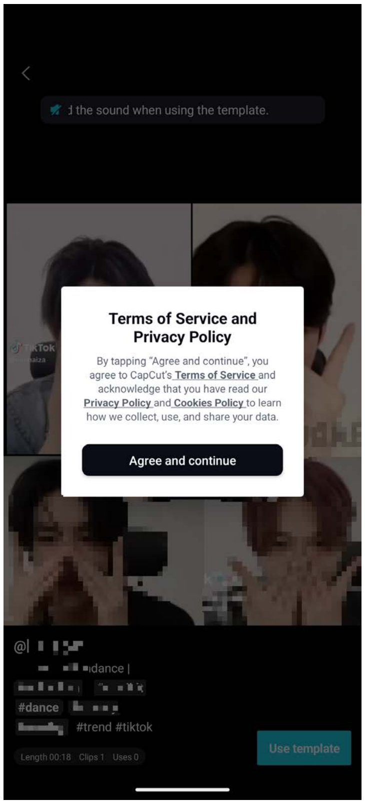


[redacted] · 2023-09-04

#CapCut #Dance #fyp #templates

#[redacted] #cripwalkhiphop

FIGURE 2B: "Terms of Service and Privacy Policy" pop-up

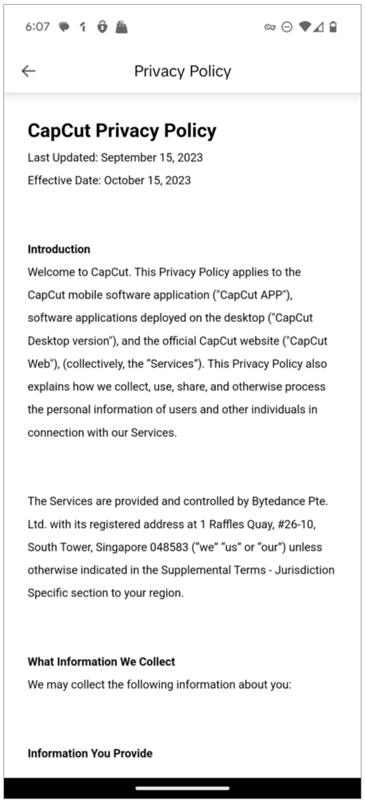


the sound when using the template.

Terms of Service and Privacy Policy

By tapping "Agree and continue", you agree to CapCut's Terms of Service and acknowledge that you have read our Privacy Policy and Cookies Policy to learn how we collect, use, and share your data.

FIGURE 2C: CapCut privacy policy



CapCut Privacy Policy

Last Updated: September 15, 2023

Effective Date: October 15, 2023

Introduction

Welcome to CapCut. This Privacy Policy applies to the CapCut mobile software application ("CapCut APP"), software applications deployed on the desktop ("CapCut Desktop version"), and the official CapCut website ("CapCut Web"), (collectively, the "Services"). This Privacy Policy also explains how we collect, use, share, and otherwise process the personal information of users and other individuals in connection with our Services.

The Services are provided and controlled by Bytedance Pte. Ltd. with its registered address at 1 Raffles Quay, #26-10, South Tower, Singapore 048583 ("we" "us" or "our") unless otherwise indicated in the Supplemental Terms - Jurisdiction Specific section to your region.

What Information We Collect

We may collect the following information about you:

Information You Provide

use, and share your data" – meaning that you are now voluntarily and directly sending your data to ByteDance. Figure 2A is a screenshot of a TikTok video that has the "CapCut – Try this template" feature embedded in it. Figure 2B is a screenshot of the modal written "Terms of Service and Privacy Policy" after clicking the CapCut template try-out. Figure 2C is a screenshot of the CapCut Privacy Policy that indicated its service is controlled by ByteDance (CapCut Privacy Policy 2023).

CapCut collects numerous amounts of data, including biometric identifiers such as face and body features and attributes (CapCut 2023) and serves as the perfect fuel for Beijing's surveillance algorithm.

In 2024, CapCut's template is not limited to dancing videos but also all other sorts of clips, subjecting more users' data to the Chinese company. Despite the statement "The Services are provided and controlled by ByteDance Pte/Ltd." being adequately clear on its Privacy policy, the reality is that few users would read or care before giving legal consent for their data to be exploited. Ignorance is the key that unlocks the door for TikTok to obtain personal data for mass surveillance and foreign information manipulation and interference (FIMI).

Threat II: Foreign information manipulation and interference (FIMI)

Chinese influence operations on TikTok: What's so special?

TikTok's Community Guidelines, under the section of Integrity and Authenticity, stated that it does not allow "inaccurate, misleading, or false content that may cause significant harm to individuals or society," as well as "misinformation about civic and electoral processes, regardless of intent" (TikTok 2023a). Yet Chinese disinformation apparently does not fall into that category.

The PRC and China-affiliated entities leverage TikTok's short reel feature – most popular in the form of a 10- to 30- second video – integrating various cognitive warfare tactics that exploit vulnerabilities in human psychology for their influence operations on the platform.

Filled with quick cuts, intense background music, and engaging visuals – these short videos effectively amplify the PRC messages while often triggering emotional responses that can be manipulated. As emotional manipulation is often based on one's fear and anxiety – impeding the brain from rational thinking – it makes one more susceptible to persuasive messages, propaganda, and disinformation.

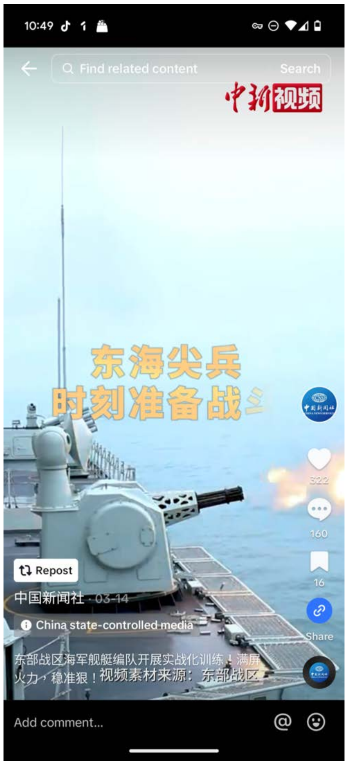
The following subsections – coercive measures, electoral interference, conspiracy theory, and rebuke of "Western lies" [1] – illustrate how the PRC utilizes TikTok for influence operations and cognitive warfare that steer public opinion – both in China, where it seeks to reshape Chinese public perception in favour of Beijing, as well as abroad, where it seeks to sow division within liberal democracies. The Tactics, Techniques, and Procedures (TTPs) deployed, as well as attribution to the PRC and/or PRC-affiliated entities, will also be examined in these case studies.

Coercive measures

Earlier this year, the China Coast Guard (CCG) conducted controversial grey zone activities around the disputed Kinmen Islands in the Taiwan Strait in an effort to challenge Taiwan's sovereignty and intimidate its citizens. At the same time, the PRC launched influence operations via TikTok to sow division in Taiwan (Lee 2024).

The PRC state media *China News Service (CNS)*, for instance, published a 16-second video titled "The Eastern Theater Command naval fleet conducts realistic combat training! Full-screen firepower, stable, accurate, and ruthless!" on TikTok (*China News Service* 2024) to amplify PLAN's capability while challenging Taipei's ability to exercise control in the restricted/prohibited waters. Focusing on missile-firing scenes with loud shooting noises, accompanied by wordings such as "the Eastern Theater fleet is always ready to fight," the clip attempts to generate fear and distress in Taiwanese society and therefore waver public support for Taipei to confront Beijing's active challenges to the status quo by threatening war on the island.

FIGURE 3: TikTok video praising the Chinese naval fleet



中国新闻社 · 03-14

China state-controlled media

东部战区海军舰艇编队开展实战化训练！满屏火力，稳准狠！视频素材来源：东部战区

Figure 3 is a screenshot of the China News Service's TikTok video "The Eastern Theater Command naval fleet conducts realistic combat training! Full-screen firepower, stable, accurate, and ruthless!" with its highlighted line "the Eastern Theater fleet is always ready to fight."

Electoral interference

As a recent American intelligence community report noted, PRC-affiliated entities utilized TikTok to target both Republican and Democract candidates during its midterm election in 2022 (United States Office of the Director of National Intelligence 2024). To demonstrate how Beijing could leverage TikTok for electoral interference, Chinese influence operation targeting Taiwan's presidential and legislative election in January 2024 is a perfect paradigm.

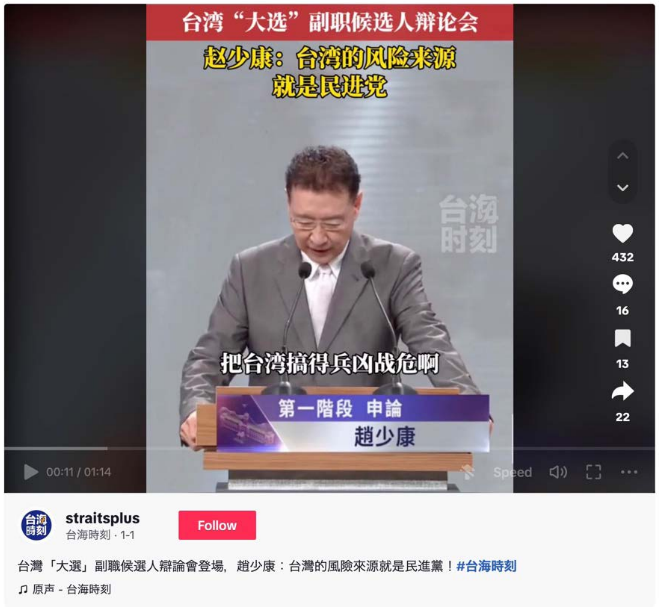
For instance, during the election cycle, *Straits Plus* (台海時刻) – a TikTok account managed by the Fujian Provincial Radio and Television Bureau (福建省广播电视局), which is under the direct control of the Fujian provincial government (The People's Government of Fujian Province, PRC 2024) – published multiple videos to defame the Democratic Progressive Party (DPP). As the *Straits Plus* has no labelling (TikTok has the labelling feature for state-controlled media) nor information in the bio section indicating its state affiliation, it misled audiences by falsifying an impression that it is an independent media presenting its stance when it had repeatedly amplified Beijing's narrative of "Taiwan is in a state of war and danger" (台灣兵凶戰危) and that DPP administration is responsible for the "crisis."

Moreover, *Straits Plus* also cited Vice Presidential candidate Jaw Shau-Kong (趙少康)'s comment – which aligned with their rolling narrative "Taiwan strait crisis was created by DPP" – edited it into a short reel and fuelled it on TikTok (*Straits Plus* 2024). Additionally, it helped to amplify certain presidential candidates' speeches that were more in line with Beijing's interests. When Taiwan had its first televised debate, *Straits Plus* created videos that highlighted the two presidential candidates Hou Yu-Ih (侯友宜) and Ko Wen-Je (柯文哲)'s attack on the DDP and narratives such as cross-strait "mutual respect and cooperation" (*Straits Plus* 2023) while leaving out any comments candidate Lai Ching-te made during the debate. Figure 4 (page 22) shows *Straits Plus*'s TikTok video citing Vice Presidential candidate Jaw Shau-Kong (趙少康). "DPP made Taiwan in this state of war and danger" (台灣兵凶戰危) – which aligned with Beijing's rolling narrative. Figure 5 (page 22) shows *Straits Plus*'s TikTok videos highlighting Ko (left and middle) and Hou (right), two presidential candidates whose narratives align with Beijing's, as they attack candidate Lai and DPP, and/or advocate for cross-strait "mutual respect and cooperation."

These operations attempted to influence public opinion (in this case, against Lai and the DPP) during elections has seriously undermined the liberal democratic process.

State-affiliated accounts that participated in the operation are China's best propaganda machine as there is no balanced reporting nor fairness for any political candidates to promote their campaign given its censored system and the PRC-affiliated nature. TikTok can fuel any candidates' account as Beijing sees fit with their "For You Feed" (FYF) or "Explore" recommendation algorithm.

FIGURE 4: *Straits Plus*'s TikTok video of Taiwanese Vice Presidential candidate Jaw Shau-Kong

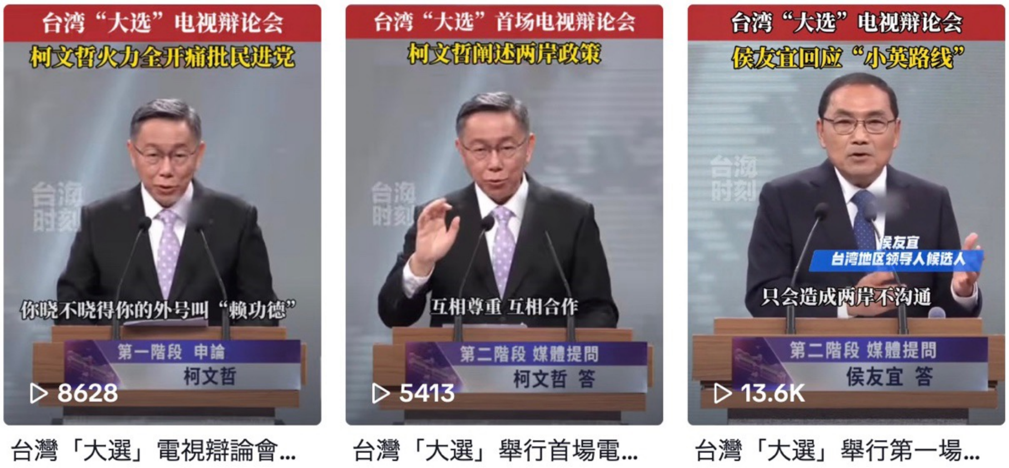


straitsplus
台海時刻 · 1-1

台灣「大選」副職候選人辯論會登場，趙少康：台灣的風險來源就是民進黨！#台海時刻

♫ 原声 - 台海時刻

FIGURE 5: *Straits Plus*'s TikTok videos showing pro-Beijing presidential candidates attacking Lai and the DPP



台灣「大選」電視辯論會...

台灣「大選」舉行首場電...

台灣「大選」舉行第一場...

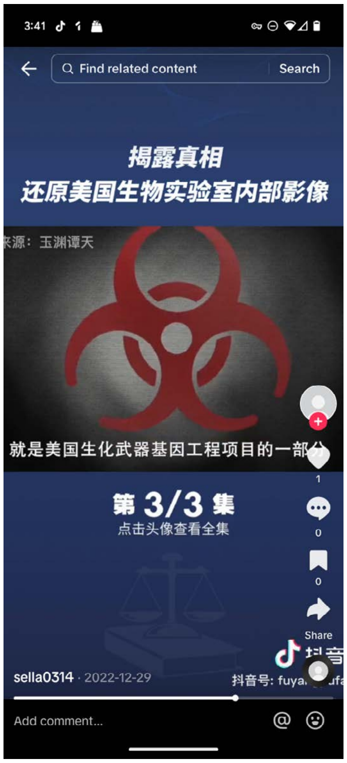
Despite the series of disinformation campaigns, they did not make a visible impact on Lai's victory in the presidential election. However, influence operations that utilize TikTok as a tool as well as other tactics can still potentially impact election outcomes, especially if the races are close.

Conspiracy theories

Conspiracy theories are one of the most common types of disinformation the PRC utilizes TikTok for as a dissemination and amplification tool. From "the US created the COVID-19 virus," to supposed electoral fraud in Taiwan's election, or to allegations that Hong Kong protestors are funded by the CIA – conspiracy theories that align with Beijing's narratives and political agendas are constantly being shared on TikTok.

For instance, TikTok user "@sella0314" published a series of three videos under the headline of "Revealing the truth – Reconstructing the internal video footage of the American biological laboratory." The videos implied that Ralph Baric – a virologist at the US National Academy of Science – "created covid-19 virus" and that his research is "a part of America's genetic engineering project." The video appears to have originated from the Douyin (Chinese version of TikTok) account *Fuyangpufa* (阜阳普法), which is the official account of *Fuyang City Bureau of Justice* (阜阳市司法局). In addition, the watermark in the video also states its source – *Yuyuan Tantian* (玉渊谭天) – which is a sock puppet account of PRC state media *China Central Television* (CCTV). This conspiracy narrative also aligns with Ministry of Foreign Affairs of China Spokesperson Wang Wenbin's claim that "an investigation into Baric's team and his lab would clarify whether or not there is research on coronaviruses and whether they could produce COVID-19" (Xinhua 2021).

FIGURE 6: Example of COVID-19 disinformation on TikTok



揭露真相
还原美国生物实验室内部影像

来源：玉渊谭天

就是美国生化武器基因工程项目的一部分

第 3/3 集
点击头像查看全集

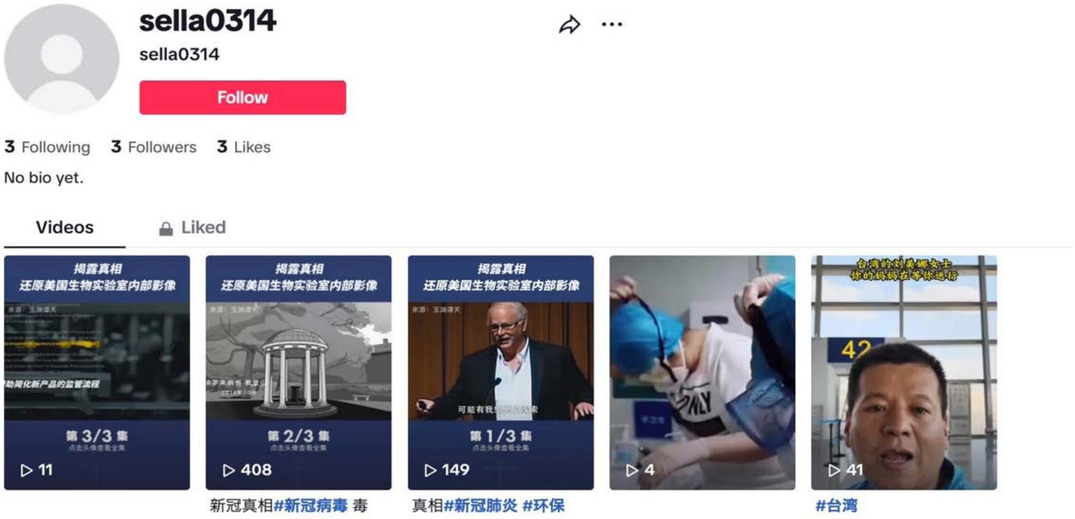
sella0314 · 2022-12-29

抖音号: fuya

Figure 6 shows the third episode of the series of videos published by the TikTok user @sella0314 titled "Revealing the truth: Reconstructing the internal video footage of the American biological laboratory."

This @sella0314 TikTok account had only published 5 videos, which all had December 2022 timestamps. It had a mere three followers and three following accounts. The title for its first episode of the series included

FIGURE 7: Probable fake account



sella0314

sella0314

Follow

3 Following 3 Followers 3 Likes

No bio yet.

Videos Liked

新冠真相#新冠病毒 毒

真相#新冠肺炎 #环保

#台湾

an irrelevant hashtag #environmental friendly (#环保) while its second had a duplicated Chinese character “COVID Truth #COVIDVirus Virus (新冠真相 #新冠病毒 毒). This indicates that it is likely a spam account created to spread the PRC-aligned narratives. Regardless of its actual ties with the PRC, it is a clear example of TikTok flooded with conspiracy theories based on PRC state media, government entities, and official claims. Figure 7 is a screenshot of the profile of the TikTok user @sella0314, which is likely a spam account.

Additionally, since TikTok videos are often very short (sometimes just a few seconds), there is little time for critical thinking, just quick consumption with a limited attention span, which, over time, can lead to greater susceptibility to PRC influence campaigns. Since many viewers won’t realize the videos are part of a targeted disinformation campaign, it greatly enhances the effectiveness of IOs to sow confusion, polarize public debate, and fuel extremism.

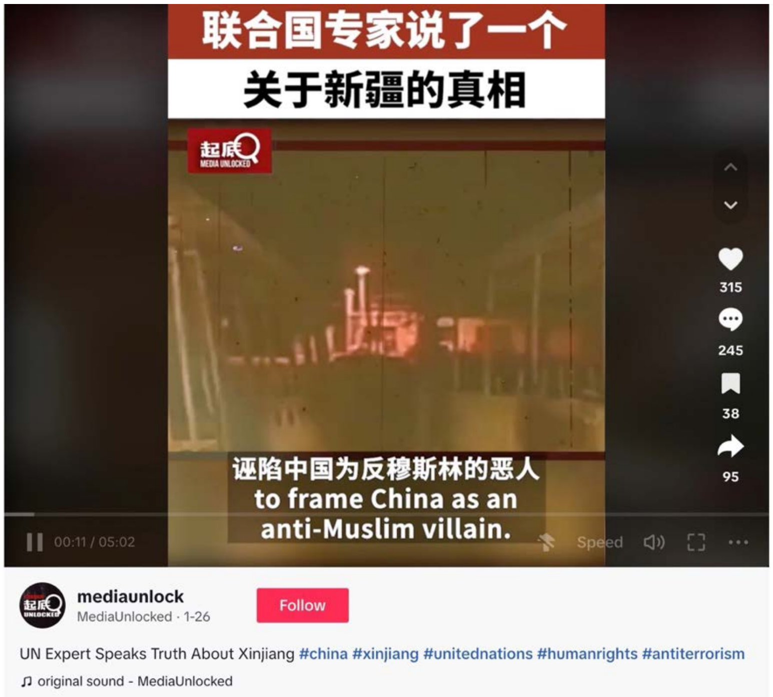
Protecting China’s image: Rebuke of “Western lies”

Perhaps what is most special about TikTok remains its affiliation with the Cyberspace Administration of China (CAC) [details in “TikTok’s significance to Beijing,” page 11]. As the CAC’s main role is to manipulate information space, especially regarding negative international opinion of China, TikTok happens to be the best strategic tool for disseminating propaganda materials that rebuke Western countries' "smears" of the PRC.

The TikTok account "Media Unlocked," for instance, published multiple videos that "debunk" Western "lies." For instance, it published a TikTok video titled "UN Expert Speaks Truth About Xinjiang" – claiming that "Western governments have long denied that Xinjiang suffers from a terrorism problem and have tried to manipulate the UN human rights system to frame China as an anti-Muslim villain" (Media Unlocked 2024). Media Unlocked is operated by PRC-affiliated media *China Daily*. Yet the only information available on its TikTok profile is that they are "China-based journalists covering China & Global Issues." Figure 8 below shows Media Unlock's TikTok video "UN Expert Speaks Truth About Xinjiang."

Another prominent example is Key Opinion Leader (KOL) Li Jingjing's TikTok video "Western lies about Xinjiang are falling apart, piece by piece" (Li 2023). She rebuked various accusations regarding Xinjiang's forced labour in her video. Li Jingjing is a journalist at the PRC-state media *Chinese Global Television Network (CGTN)*; however, her account has no state-

FIGURE 8: Example of a rebuke of "Western lies" on TikTok about Xinjiang

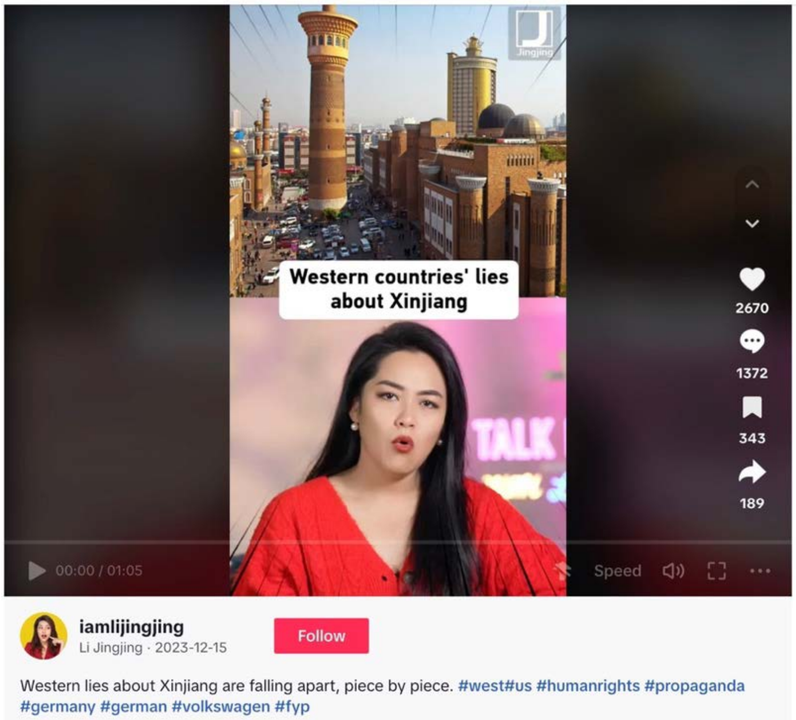


mediaunlock
MediaUnlocked · 1-26

UN Expert Speaks Truth About Xinjiang #china #xinjiang #unitednations #humanrights #antiterrorism

♫ original sound - MediaUnlocked

FIGURE 9: Second example of a rebuke of “Western lies” on TikTok about Xinjiang



Western countries' lies about Xinjiang

iamlijingjing
Li Jingjing · 2023-12-15

Western lies about Xinjiang are falling apart, piece by piece. #west#us #humanrights #propaganda #germany #german #volkswagen #fyp

affiliation label and her profile biography only noted that she is a “Chinese journalist” that “bring(s) you a different perspective on world news.” Figure 9 is screenshot of Li Jingjing’s TikTok video “Western lies about Xinjiang are falling apart, piece by piece.”

These videos are all accompanied by English audio and/or subtitles – likely targeting TikTok users worldwide. IOs that target international audiences help to sow confusion and divide public opinion by creating an alternative narrative. This is especially effective on people who have no prior knowledge of the issue and are subjected to repeated exposure.

TikTok’s “For You” algorithm

In addition, TikTok had partially shared server codes with Douyin as they are both developed by ByteDance – and these codes, which determine the platform’s algorithm, are likely subjected to the PRC’s regulations on internet censorship and its recommendation algorithm.

In December 2019, the CAC announced the "Provisions on the Governance of the Online Information Content Ecosystem" (网络信息内容生态治理规定) – a new set of internet censorship regulations (Cyberspace Administration of China 2019). On one hand, the regulation encourages content producers to create, duplicate, and disseminate articles that "promote Xi Jinping's thought" on "Socialism with Chinese Characteristics" and positive messages that showcase "the uplifting spirit" of the Chinese nation and culture. On the other hand, it also focuses on cracking down on content that "endanger national security, leak state secrets, subvert state power, undermine national unity," as well as "hamper national honour and interests."

Moreover, in December 2021,[2] with the signatories of the Ministry of Industry and Information Technology and the MPS, the CAC also announced the "Provisions on the Management of Algorithm Recommendations in Internet Information Services" (互联网信息服务算法推荐管理规定) that mandate recommendation algorithm service providers to "actively transmit positive energy" and cannot recommend contents that "threaten national security and public interest," or "disrupt economic and social order" (Government of the People's Republic of China 2021).

These legislations and regulations revealed Beijing's struggles in dealing with emerging technologies. While the PRC fears unregulated algorithm recommendations based on users' interests and genuine engagement will shake its control over the information space – as it might not amplify pro-Beijing propaganda and/or even anti-Beijing narratives – China is also eager to leverage AI-governance both at home and abroad to amplify its political agendas (Sheehan 2022). In fact, the evolving regulations showcased Beijing's urgency and ambition to utilize recommendation algorithms for its influence operations.

As all Chinese social media companies are obliged to PRC's provisions, these regulation principles would need to be embedded into ByteDance's algorithm – if they haven't been already. And ByteDance developed the algorithms for both TikTok and Douyin (Shepardson and Wang 2022). Previously, Reuters has reported that while the code that determines the look and feel of TikTok has been separated from Douyin, the server code of TikTok – which is the heart of the algorithms for content moderation and recommendation, as well as data storage and user profiles management – is still partially shared across other ByteDance products.

In short, TikTok's "For You" algorithm likely amplifies PRC propaganda and censors "negative" content for international users by using shared server codes with ByteDance/Douyin.

ByteDance's willingness to obey Beijing stems in part from a previous PRC crackdown against the company's news app Toutiao in 2016. At the time, ByteDance founder Zhang Yiming had disavowed the notion of needing an "editor-in-chief" to "guide users and/or inculcate any 'values' in them.'" Following the crackdown – the CAC ordered app stores to block all downloads of Toutiao for three weeks – Zhang publicly apologized and vowed to ensure that its recommendation algorithms would promote PRC propaganda. (Sheehan 2022; Ryan, Fritz, and Impiombato 2020). The fear of a second and likely worse crackdown is a key motivator driving Byte/Dance's willingness to comply with the PRC.

The case studies examined here highlight TikTok's role as a key vehicle for disseminating PRC propaganda. Despite the company's claims to the contrary, TikTok is not "independent."

Implications for Canada

Given its status as a member of the Five Eyes multilateral intelligence sharing alliance (FVEY), Canada is and will always be a major target of the PRC. The relationship between the two countries has been especially fraught since 2018, when two Canadian citizens, Michael Kovrig and Michael Spavor, were arrested by China and accused of espionage. Held for 1,019 days, the "Two Michaels" were released on September 24, 2021. Their detention by China was generally seen as punishment for Canada's arrest in December 2018 of Huawei CFO Meng Wanzhou, who was wanted in the US for alleged bank and wire fraud. In 2022, the relationship was further strained when Canada banned Chinese tech giant Huawei from using its 5G network due to national security concerns. Since the Huawei and Two Michaels incidents, more conflicts around national interests and liberal democratic values have evolved between the two states – and with Canada-China relations worsening – Ottawa is being more frequently targeted (Tunney and Raycraft 2022; Austen and Isai 2024).

Examples of recent PRC IOs against Canada include:

- videos accusing the Two Michaels of being spies, thereby justifying their arbitrary arrest in China;
- articles denouncing a Canadian MP's claim of being coerced by the PRC as nothing but "political hype;" and
- posts claiming that Canada was "intruding on China's territorial seas and airspace" and/or attacking the credibility of a Canadian journalist who reported on PLA jets intercepting a Canadian surveillance plane engaged in a legitimate operation in international air space.

The list goes on – and will not stop until Ottawa takes concrete actions to counter these malign foreign information manipulation and interference.

PRC IOs are also targeting Canada and other liberal democracies in an effort to undermine support for countries and territories being oppressed by authoritarianism, such as Ukraine, Taiwan, Xinjiang, and Hong Kong.

While there are several major Canadian media outlets on TikTok, including CTV News (1.2 million followers, 41.3 million likes) and CBC News (571,000 followers, 13 million likes), these outlets simply cannot compete with TikTok's algorithm when the PRC intends to manipulate the information space. TikTok could censor content via pre-upload or other keyword filter systems, limiting the reach of valid and accurate content via the feed's recommendation algorithm. Another censorship tactic is shadow banning – a moderation practice of covertly restricting users' content visibility without completely banning them. During shadow banning, content is often still visible to users, therefore they often don't know that their content is being restricted. This occurs often on Chinese social media platforms such as Weibo and WeChat.

TikTok's supporters often try to frame legitimate concerns as nothing more than paranoia. However, the truth is, TikTok presents a prominent threat to national security and liberal democracy.

In addition, Canada's ongoing Public Inquiry Into Foreign Interference in Federal Electoral Processes and Democratic Institutions (Foreign Interference Commission 2024) has also revealed that Beijing's electoral interference, influence operations (IOs), and other hybrid threats posed to our democratic institutions are far from imagination and on a much greater and comprehensive scale than mere TikTok – and Ottawa is a thousand steps behind enforcing effective countermeasures.

Policy recommendations

Beijing's hybrid warfare strategies operate in multiple domains – and the data it mines helps support its grand strategy of leveraging data for economic and strategic purposes. The PRC would not hesitate to exploit any means that could undermine its adversaries. Therefore, one should assume that the data of all China-linked companies is being exposed, harvested, and utilized for the PRC's political agendas, including influence operations and digital surveillance.

TikTok: Divest or face ban

Despite the recently passed *Protecting Americans from Foreign Adversary Controlled Applications Act* in the US often being called the "TikTok ban," it is not a direct ban but measures to force TikTok's parent company ByteDance to divest it or face a ban on all app stores (United States Congress 2024). The goal is to cut the platform's ties with Beijing, halting the flood of data pouring into the PRC and stifling Chinese influence operations. This approach is a good approach for other like-minded democracies to consider.

For Canada, the procedure is even simpler. The *Investment Canada Act (Part IV.1) ('the Act')* details the application of "Investments injurious to National Security" (Government of Canada 1985) and to determine whether the company falls into that category, *The Guidelines on the National Security Review of Investments (Paragraph 8 (ix))* was issued under section 38 of the Act. The latter stated that "the potential impact of the investment on Canada's international interests including foreign relationships" could be considered by the Minister of Innovation, Science and Industry or Governor-in-Council in relation to national security (Government of Canada 2021).

In other words, Ottawa could initiate the enforcement of ByteDance's divestiture from TikTok or a ban (if it refuses or fails to divest), without bringing in new legislation.

Given TikTok's distinctive significance as Beijing's strategic tool – featuring a strong global user base in a multilingual setting – it would be difficult, if not, impossible for other PRC social media platforms like Weibo and WeChat (which are designated for Chinese-language speakers) to replace it in the near future. Hence, compelling TikTok to divest from its Beijing-based parent company will be an effective short-term solution to the burning issue of protecting our sensitive data from China, as well as mitigating other risks such as digital surveillance and electoral interference.

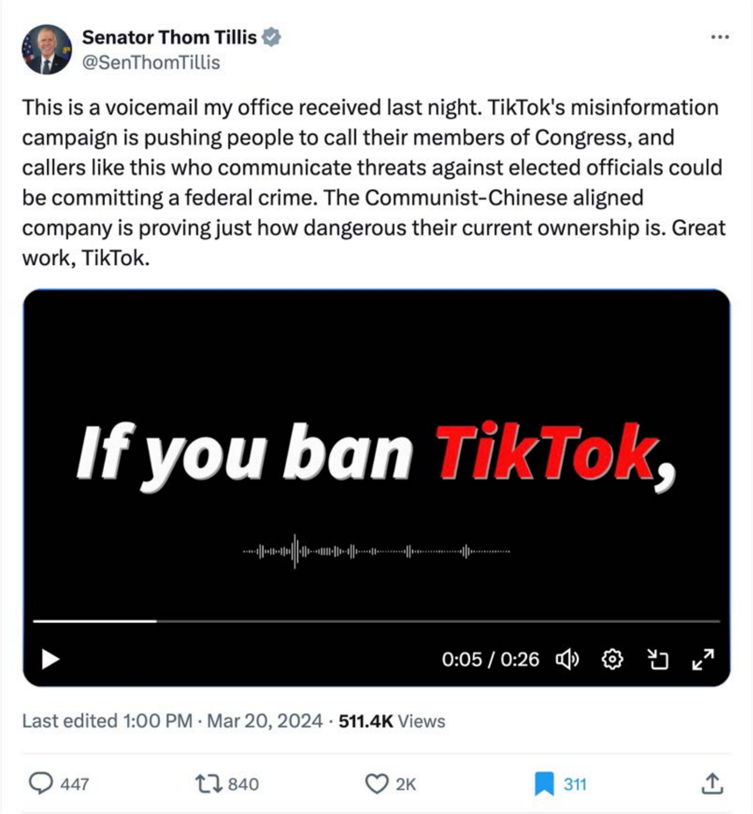
> *Canada (has) banned TikTok from government devices.*

In the past two years, Canada, the United Kingdom, Australia, Taiwan, New Zealand, and the European Union (European Parliament, European Commission, and European Council) have banned TikTok from government devices, and some have also advanced the ban to devices that connect to their parliamentary networks (Hassan et al. 2024). As Western democracies have conducted in-depth research and enacted security measures on TikTok's significant threat posed to privacy and security, these actions have set precedents for more rigorous countermeasures.

Prime Minister Justin Trudeau has said that the TikTok ban on government devices was "maybe the only step" the government would need to take (Raycraft 2023). However, it is clear more action is needed. Evidence of this was displayed recently during a TikTok IO campaign intended to convince, or possibly intimidate, American lawmakers into halting the "TikTok ban."

In March 2024, TikTok CEO Chew Shou-Zi posted a video urging American citizens to call their representatives in the US Congress to voice opposition to the potential ban. Lawmakers' offices were immediately flooded with calls from TikTok users, some of whom threatened violence against the lawmakers. For instance, Senator Thom Tillis received a death threat via voicemail, vowing "If you ban TikTok, I will find you and shoot you" (Tillis

FIGURE 10: Threatening emails to Ottawa targets



Senator Thom Tillis @SenThomTillis

This is a voicemail my office received last night. TikTok's misinformation campaign is pushing people to call their members of Congress, and callers like this who communicate threats against elected officials could be committing a federal crime. The Communist-Chinese aligned company is proving just how dangerous their current ownership is. Great work, TikTok.

Last edited 1:00 PM · Mar 20, 2024 · **511.4K** Views

2024). During the campaign TikTok also sent push alerts to users urging them to lobby Congress in their favour. Figure 10 is a screenshot of Senator Thom Tillis's tweet, which included a threatening voicemail.

Additionally, TikTok recruited dozens of its content creators to travel to Washington, DC, where they met with lawmakers and posted videos to fight the bill in Congress with the hashtag #KeepTikTok (Maheshwari and McCabe 2024b).

The world witnessed how TikTok flaunted its political mobilization power, and are now aware of its determination to use it when necessary. This is an extremely alarming situation – given TikTok's ties with the Chinese government, the PRC could mobilize TikTok users for protests, to threaten and harass individuals, and even for extreme actions for its political and strategic agendas on foreign soil.

Like-minded democracies need to urgently move on action-oriented policies to safeguard our national security and liberty.

Laws and regulations for cross-border data transfer to foreign adversaries and data brokers

It is important to understand that banning TikTok, or forcing its divestiture, is just a short-term solution (Wang and Dave 2020) – there will always be another TikTok, and the world does not lack social media platforms that threaten national and individual security. Besides, TikTok users could always resort to VPNs to bypass restrictions and continue using the service. To combat FIMI and address privacy concerns in the post-digital era, liberal democracies need something more permanent.

As discussed in previous sections, companies with Chinese affiliations, no matter how subtle the ties are, are obliged by law to hand over their data to the Chinese authorities – regardless whether the data are collected in China or on foreign soil. Therefore, the only way to permanently mitigate the threat is to prevent cross-border data transfers to foreign adversaries.

First, a robust framework should be established for security audits. This is to assess the risk posed by software applications affiliated with the PRC, amongst other foreign adversaries, to national security, foreign policy, information integrity, as well as to individual security, fundamental freedoms, and liberal democratic values.

Next, we need concrete policies with strong enforcement mechanisms to prevent and deter these entities from transporting our data to the PRC. The US *Protecting Americans from Foreign Adversary Controlled Applications Act* is an example of a good first step. However, there are additional measures that can be used to compel companies to cut ties with PRC-linked entities, such as official statements to blacklist them (with press coverage to "name and shame"), as well as financial penalties for tech companies or app stores that violate restrictions by allowing downloads from their platforms.

The risk assessment framework could also be applied to data brokers. As lawmakers scrutinize relevant laws and regulations to tighten the current practices of allowing citizens' data to be brought and transferred to the PRC legally, a comprehensive legal framework could be established to mitigate risks posed by the PRC getting its hands on foreign entities' sensitive information.

While legal procedures take time and require progressive effort, they should be initiated sooner rather than later. At the very least, government bodies should begin reviewing their current options for tightening restrictions on cross-border data transfer to foreign adversaries.

Universal transparency practices with Very Large Online Platforms (VLOPs)

Governments should work with social media platforms, VLOPs in particular, to establish universal transparency practices (Chandra and Chao 2023). This may include a mandatory scheme to label state-affiliated entities, conduct investigations, and report on influence operations and cyberattacks detected.

Like-minded democracies could also pressure VLOPs for other non-mandatory but highly recommended measures such as allowing more access for researchers to the platforms' Application Programming Interface (API) and building a robust system for civil society to report suspicious activities such as state-sponsored disinformation campaigns, coordinated inauthentic behaviours, and other influence operations.

Bolstering democratic resilience

Indubitably, defending democracy cannot rely solely on governmental policy or institutional changes. The effectiveness of laws and regulations is limited if the people themselves are not willing to be protected. We need to strengthen democratic resilience – i.e., the public's awareness and determination to protect their personal data from being exploited or influenced by malign actors. Only education and media literacy would be able to foster that.

Finland's anti-fake news initiative since 2014 is a salient example of teaching students, journalists, politicians, and ordinary citizens how to counter disinformation that is designated to sow confusion and magnify division in society (Mackintosh 2019). Taiwan's decentralized network also presents a compelling model of how to foster a culture of grassroots civic tech engagement and formulate a comprehensive approach to strengthening public resilience (Lee 2024a).

Conclusion

Perhaps one of the common arguments for opposing a "TikTok ban" is that other VLOPs also collect users' data and conduct surveillance in similar ways (Thomas 2024). However, this paper has highlighted the kinds of data harvested by TikTok that are typically not gathered by Western VLOPS. Besides, the latter's data are generally not sent to totalitarian countries that conduct surveillance, or harass and coerce individuals to advance their political agendas. The other key difference is their transparency – Western VLOPs like Facebook and X publish regular transparency reports, and work with government entities and think tanks when influence operations are discovered. They also are making voluntary commitments to ensure users' privacy and safety, such as by managing the risk posed by AI technologies (The White House 2023).

This is not to say that Western VLOPs pose no risk to mass surveillance. However, in liberal democracies, there is an increased likelihood that they can be encouraged to follow proper practices via legislation and regulation, along with oversight by the Fourth Estate: the press.

As this paper has shown, Beijing employs TikTok to advance its political narratives and strategic agendas. The user data harvested by TikTok could provide priceless economic and political benefits while fuelling the PRC's mass surveillance technologies. In parallel, PRC influence operations, integrated with cognitive warfare tactics, manipulate TikTok's information environment to sow division and steer public opinion in support of Beijing and its strategic goals.

Meanwhile, TikTok's efforts to weaponize its users in its fight against the US "TikTok ban" flaunted its alarming political mobilization capability and exemplified the fact that it (and the PRC) would not hesitate to utilize such power to incite conflicts, magnify division, or even fuel extreme actions to fulfil its political agendas on foreign soil.

TikTok's extensive political leverage around the globe constitutes a valuable strategic asset for Beijing– threatening individuals and international security in like-minded democracies whenever and wherever they want. Liberal democracies have no time to waste.

The clock is ticking – not on TikTok, but on us – to safeguard our own security and sovereignty.

About the author

Sze-Fung Lee (ze/zir) is an independent researcher specializing in Chinese hybrid warfare, including foreign information manipulation and interference (FIMI), grand strategy, nuclear proliferation, grey zone tactics, and cognitive warfare. Zir research also focuses on Indo-Pacific security policy, challenges posed by emerging technologies, and the politics of Hong Kong. Zir work has been featured in international media, such as the *Diplomat*, *Modern Diplomacy*, *Eurasia Review*, the *Hill Times*, *Policy Option*, and *Hong Kong Economic Journal*. Previously, ze was an analyst at the Centre for International Digital Policy, Global Affairs Canada (Ministry of Foreign Affairs) from 2022 to 2023. Ze also holds a master's degree in international security from the University of Warwick. Find ze on X/Twitter: @imleeszefung

References

Austen, Ian and Vjosa Isai. 2024. “Canadian Jailed by China in Tit-for-Tat Dispute Gets a Settlement.” *The New York Times*, March 7, 2024. Available at https://www.nytimes.com/2024/03/07/world/americas/michael-spavor-canada-china.html.

Baker-White, Emily. 2022. “Leaked Audio From 80 Internal TikTok Meetings Shows That US User Data Has Been Repeatedly Accessed From China.” BuzzFeed News. Available at: https://www.buzzfeednews.com/article/emilybakerwhite/tiktok-tapes-us-user-data-china-bytedance-access.

Baker-White, Emily. 2022a. “TikTok Parent ByteDance planned to use TikTok to Monitor the Physical location of Specific American Citizens.” *Forbes*, October 20, 2022. Available at: https://www.forbes.com/sites/emilybaker-white/2022/10/20/tiktok-bytedance-surveillance-american-user-data/?sh=130828b36c2d.

Baker-White, Emily. 2022b. “TikTok Spied on Forbes Journalists.” *Forbes*, December 22, 2022. Available at: https://www.forbes.com/sites/emilybaker-white/2022/12/22/tiktok-tracks-forbes-journalists-bytedance/?sh=6e7748cf7da5.

CapCut. 2023. “CapCut Privacy Policy.” Available at: https://sf16-draftcdn-sg.ibytedtos.com/obj/ies-hotsoon-draft-sg/capcut/via_clause_privacy_policy_en.html.

Chandra, Bilva and Chao, Lev Navarre. 2023. “Dismantling the Disinformation Business of Chinese Influence Operations.” The RAND Corporation, October 17, 2023. Available at: https://www.rand.org/pubs/commentary/2023/10/dismantling-the-disinformation-business-of-chinese.html.

Charon, Paul and Jean-Baptiste Jeangène Vilmer. 2021. "Chinese Influence Operations – A Machiavellian Moment." The Institute for Strategic Research. Available at: https://www.irsem.fr/report.html.

China Central Television. 2017. "The Ministry of Finance initiate the establishment of the China Internet Investment Fund." January 23, 2017. Available at: http://m.news.cctv.com/2017/01/23/ARTI5AbujVZahlrgLsTD0lUI170123.shtml （中國中央電視台（2017）。〈中央财政发起设立中国互联网投资基金〉）

China Daily. 2015. "National Security Law of the People's Republic of China (2015) [Effective]." December 11, 2015. Available at: https://govt.chinadaily.com.cn/s/201812/11/WS5c0f1b56498eefb3fe46e8c9/national-security-law-of-the-peoples-republic-of-china-2015-effective.html.

China News Service. 2015. "Xi Jinping and the '13th Five-Year Plan' 14 Major Strategy: National Big Data Strategy." November 12, 2015. Available at: https://www.chinanews.com.cn/m/gn/2015/11-12/7620676.shtml. （中国新闻网 （2015） 。〈习近平与"十三五"十四大战略：国家大数据战略〉）

China News Service. 2024. "The Eastern Theater Command naval fleet conducts realistic combat training! Full-screen firepower, stable, accurate, and ruthless!" TikTok, March 14, 2024. Available at: https://www.tiktok.com/@chinanewsservice/video/7346068213085621511?_r=1&_t=8klgcDsLj30（中國新聞社（2024）。「东部战区海军舰艇编队开展实战化训练！满屏火力，稳准狠！」）

Cyberspace Administration of China. 2016. "The People's Republic of China Cybersecurity Law." November 7, 2016. Available at https://www.cac.gov.cn/2016-11/07/c_1119867116_2.htm (中华人民共和国国家互联网信息办公室（2016）。〈中华人民共和国网络安全法〉。)

Cyberspace Administration of China. 2019. "Cyberspace Administration of China announced the 'Provisions on the Governance of the Online Information Content Ecosystem.'" December 20, 2019. Available at: https://www.cac.gov.cn/2019-12/20/c_1578375159431916.htm （国家互联网信息办公室（2019）。〈国家互联网信息办公室发布《网络信息内容生态治理规定》〉）

Foreign Interference Commission. 2024. "Foreign Interference Commission." Accessed April 2024. Available at https://foreigninterferencecommission.ca/

Fowler, Kimberley. 2024. “Canadian content creators react to potential TikTok ban after U.S. House passed bill over security concerns.” CTV News, March 14. Available at: https://ottawa.ctvnews.ca/canadian-content-creators-react-to-potential-tiktok-ban-after-u-s-house-passed-bill-over-security-concerns-1.6808320.

Gleeson, Sean. 2019. “Facial Recognition” Towers in Hong Kong? How smart are Hong Kong’s lampposts.” AFP, September 4. Available at: https://factcheck.afp.com/how-smart-are-hong-kongs-lampposts.

Government of Canada. 1985. *Investment Canada Act*. Available at: https://laws-lois.justice.gc.ca/eng/acts/i-21.8/page-4.html#h-278745.

Government of Canada. 2021. “The Guidelines on the National Security Review of Investments.” March 24, 2021. Available at: https://ised-isde.canada.ca/site/investment-canada-act/en/investment-canada-act/guidelines/guidelines-national-security-review-investments.

Government of the People’s Republic of China. 2021. “Provisions on the Management of Algorithm Recommendations in Internet Information Services.” Available at: https://www.gov.cn/zhengce/zhengceku/2022-01/04/content_5666429.htm. （中华人民共和国中央人民政府（2021）。〈互联网信息服务算法推荐管理规定〉）

Hassan, Jennifer, Ellen Francis, Ruby Mellen, and Adam Taylor. 2024. “The U.S. could ban TikTok. These countries have blocked or restricted it.” *Washington Post,* March 13, 2024. Available at: https://www.washingtonpost.com/world/2024/03/13/tiktok-ban-countries-restrictions/.

He, Laura. 2024. “Wait, is TikTok really Chinese?.” CNN, March 28, 2024. Available at: https://www.cnn.com/2024/03/18/tech/tiktok-bytedance-china-ownership-intl-hnk/index.html#:~:text=ByteDance%20was%20founded%20in%202012,the%20Chinese%20capital%20since%20then.

Hung, Tzu-Chieh and Hung, Tzu-Wei. 2020. “How China’s Cognitive Warfare Works: A Frontline Perspective of Taiwan’s Anti-Disinformation Wars.” *Journal of Global Security Studies*, 7(4), 2020, 1-18. Available at: https://academic.oup.com/jogss/article/7/4/ogac016/6647447.

Kern, Rebecca and Bordelon, Brendan. 2024. “Angry TikTok Users are still flooding Congress with calls.” Politico, March 11, 2024. Available at: https://www.politico.com/news/2024/03/11/tiktok-continues-push-alert-campaign-00146343.

Knockel, Jeffrey, Christopher Parsons, Lotus Ruan, Ruohan Xiong, Jedidiah Crandall, and Ron Deibert. 2020. "One App, Two Systems: How WeChat uses one censorship policy in China and another internationally." Citizen Lab, May 7, 2020. Available at: https://citizenlab.ca/2020/05/we-chat-they-watch/.

Lee, Sze-Fung. 2024. "Decoding Beijing's Gray Zone Tactics: China Coast Guard Activities and the Redefinition of Conflict in the Taiwan Strait." Global Taiwan Institute. Available at: https://globaltaiwan.org/2024/03/decoding-beijings-gray-zone-tactics-china-coast-guard-activities-and-the-redefinition-of-conflict-in-the-taiwan-strait/.

Lee, Sze-Fung. 2024a. "Ten Things Taiwan can Teach Canada." The Macdonald-Laurier Institute, February 22, 2024. Available at: https://macdonaldlaurier.ca/ten-things-taiwan-can-teach-canada-sze-fung-lee/.

Levine, Alexandra. 2023. "TikTok Confirms Some U.S. User Data Is Stored In China." *Forbes*, June 21. Available at: https://www.forbes.com/sites/alexandralevine/2023/06/21/tiktok-confirms-data-china-bytedance-security-cfius/?sh=4adc7ab53270.

Li, Jingjing. 2023. "Western lies about Xinjiang are falling apart, piece by piece." TikTok, December 15, 2023. Available at: https://www.tiktok.com/@iamlijingjing/video/7312822428080606507?_r=1&_t=8klmsLUDCdB.

Mackintosh, Eliza. 2019. "Finland is winning the war on fake news. What it's learned may be crucial to Western democracy." CNN Special Report accessed April 2024. Available at: https://edition.cnn.com/interactive/2019/05/europe/finland-fake-news-intl/.

Maheshwari, Sapna. 2023. "Topics Suppressed in China Are Underrepresented on TikTok, Study Says." *The New York Times,* December 21, 2023. Available at: https://www.nytimes.com/2023/12/21/business/tiktok-china.html?campaign_id=9&emc=edit_nn_20240313&instance_id=117480&nl=the-morning&regi_id=204845736&segment_id=160629&te=1&user_id=1945316c5c9fd470959a026f1a9cc108.

Maheshwari, Sapna, and McCabe, David. 2024a. "Congress Passed a Bill That Could Ban TikTok. Now Comes the Hard Part." *The New York Times*. April 23, 2024. Available at: https://www.nytimes.com/2024/04/23/technology/bytedance-tiktok-ban-bill.html.

Maheshwari, Sapna and McCabe, David. 2024b. "TikTok Prompts Users to Call Congress to Fight Possible Ban." *The New York Times,* March 07, 2024. Available at: https://www.nytimes.com/2024/03/07/business/tiktok-phone-calls-congress.html.

Media Unlocked. 2024. "UN Expert Speaks Truth About Xinjiang." TikTok, January 26, 2024 [note: labelled "Currently Unavailable" as of April 2024]. Available at https://www.tiktok.com/@mediaunlock/video/7328621672997784878?_r=1&_t=8klowsIfiRq

Nimmo, Ben, C. Shawn Eib, and L. Tamora. 2019. "Cross-Platform Spam Network Targeted Hong Kong Protest." *Graphika,* September 25, 2019. Available at: https://graphika.com/reports/spamouflage.

People's Daily. 2019. "Telling the new era police officers' stories well, National Public Security organs joined the new media Toutiao and Douyin." April 25, 2019. Available at: http://legal.people.com.cn/n1/2019/0425/c42510-31050146.html（人民网（2019）。〈讲好新时代警察故事　全国公安新媒体矩阵入驻头条抖音〉）

Poulsen, Kelvin, and McMillan, Robert. 2020. "TikTok Tracked User Data Using Tactic Banned by Google." *The Wall Street Journal.* Available at: https://www.wsj.com/articles/tiktok-tracked-user-data-using-tactic-banned-by-google-11597176738.

Raycraft, Richard. 2023. "Federal government banning social media platform TikTok from government phones." CBC News, February 27, 2023. Available at: https://www.cbc.ca/news/politics/government-tiktok-phones-ban-1.6761737.

Ruan, Lotus, Jeffrey Knockel, and Masashi Crete-Nishihata. 2020. "Censored Contagion – How Information on the Coronavirus is Managed on Chinese Social Media." Citizen Lab, March 3, 2020. Available at https://citizenlab.ca/2020/03/censored-contagion-how-information-on-the-coronavirus-is-managed-on-chinese-social-media/.

Ryan, Fergus, Audrey Fritz, and Daria Impiombato. 2020. "TikTok and WeChat." Australia Strategic Policy Institute, September 8, 2020. Available at: https://www.aspi.org.au/report/tiktok-wechat.

Sheehan, Matt. 2022. "Tracing the Roots of China's AI Regulations." Carnegie Endowment for international Peace, February 27, 2022. Available at: https://carnegieendowment.org/2024/02/27/tracing-roots-of-china-s-ai-regulations-pub-91815.

Shepardson, David. 2023. “TikTok CEO: App has never shared US data with Chinese government.” Reuters, March 21, 2023. Available at: https://www.reuters.com/technology/tiktok-ceo-app-has-never-shared-us-data-with-chinese-goverment-2023-03-22/#:~:text=%22TikTok%20has%20never%20shared%2C%20or,Representatives%20Energy%20and%20Commerce%20Committee.

Shepardson, David and Echo Wang. 2022. “TikTok seeks to reassure U.S. lawmakers on data security.” Reuters, July 1, 2022. Available at: https://www.reuters.com/business/media-telecom/tiktok-seeks-reassure-lawmakers-us-data-security-2022-07-01/.

Southern Metropolis Daily. 2018. “National cyber police departments collectively create accounts on Douyin and will establish a ‘One-Click Reporting by Cyber Police’ mechanism.” September 14, 2018. Available at: https://www.sohu.com/a/253861358_161795（南方都市报（2018）。〈全国网警部门集体在抖音开账号，将建“网警一键举报”机制〉）

Straits Plus. 2023. “Taiwan ‘General Election’ holds its first TV debate, Ko Wen-Je elaborates on the cross-strait policy.” TikTok, December 30, 2023. Available at: https://www.tiktok.com/@straitsplus/video/7318403718200823041 （台海時刻（2023）。「台灣「大選」舉行首場電視辯論會，柯文哲闡述兩岸政策。」）

Straits Plus. 2024. “Taiwan ‘General Election’ vice-presidential candidate debate kicks off, Jaw Shau-Kong: The source of Taiwan’s crisis is the Democratic Progressive Party!” TikTok, January 1, 2024. Available at: https://www.tiktok.com/@straitsplus/video/7319151156524043522?_r=1&_t=8kllQy2UXqw (台海時刻（2024）。「台灣「大選」副職候選人辯論會登場，趙少康：台灣的風險來源就是民進黨！」）

Takeshi, Kihara. 2019. “Hong Kongers wreck smart lamppost on surveillance fears.” *Nikkei Asia*, August 29. Available at: https://asia.nikkei.com/Spotlight/Hong-Kong-protests/Hong-Kongers-wreck-smart-lampposts-on-surveillance-fears.

The National People’s Congress. 2017. “The People’s Republic of China Intelligence Law.” June 27, 2017. Available at: http://www.npc.gov.cn/zgrdw/npc/xinwen/2017-06/27/content_2024529.htm (中国人大網（2017）。〈中华人民共和国情報法〉。)

The New York Times. 2024. “The Clock Ticks for TikTok.” March 12, 2024. Available at: https://www.nytimes.com/2024/03/12/business/dealbook/tiktok-house-ban.html.

The Paper. 2023. "The National Bureau of Data officially unveils, 50 trillion data assets 'come to life.'" Available at: https://m.thepaper.cn/newsDetail_forward_25061324（澎湃（2023）。〈国家数据局正式揭牌，50万亿数据资产"活"了〉）

The People's Government of Fujian Province, The People's Republic of China. 2024. "Government Structure." Available at: https://www.fujian.gov.cn/english/government/structure/.

The People's Republic of China. 2022. "State Council announcement 2022 Vol.9." Available at: https://www.gov.cn/gongbao/content/2022/content_5682426.htm.

The People's Republic of China, Ministry of Foreign Affairs. 2024. "Foreign Ministry Spokesperson Wang Wenbin's Regular Press Conference on April 23, 2024." April 23, 2024. Available at: https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/202404/t20240423_11287884.html.

Thomas, Elise. 2024. "Pro-CCP Spamouflage campaign experiments with new tactics targeting the US." Institute for Strategic Dialogue, April 01, 2024. Available at: https://www.isdglobal.org/digital_dispatches/pro-ccp-spamouflage-campaign-experiments-with-new-tactics-targeting-the-us/#_ftn1.

TikTok. 2023. "Privacy Policy." Available at: https://www.tiktok.com/legal/page/eea/privacy-policy/en.

TikTok. 2023a. 'Community Guidelines'. Available at https://www.tiktok.com/community-guidelines/en/integrity-authenticity/#1.

Tillis, Thom. 2024. "This is a voicemail my office received last night. TikTok's misinformation campaign is pushing people to call their members of Congress, and callers like this who communicate threats against elected officials could be committing a federal crime. The Communist-Chinese aligned company is proving just how dangerous their current ownership is. Great work, TikTok." X, March 20. Available at: https://twitter.com/SenThomTillis/status/1770495527508939255.

Tunney, Catharine and Richard Raycraft 2022. "Canada bans Chinese tech giant Huawei from 5G network." CBC News, May 19, 2022. Available at https://www.cbc.ca/news/politics/huawei-5g-decision-1.6310839.

United States Congress. 2024. "H.R.7521 - Protecting Americans from Foreign Adversary Controlled Applications Act." Available at https://www.congress.gov/bill/118th-congress/house-bill/7521.

United States Office of the Director of National Intelligence. 2024. "2024 annual threat assessment of the U.S. intelligence community." March 11, 2024. Available at: https://www.odni.gov/index.php/newsroom/reports-publications/reports-publications-2024/3787-2024-annual-threat-assessment-of-the-u-s-intelligence-community.

United States, The White House. 2023. "FACT SHEET: Biden–Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI." July 21, 2023. Available at: https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/21/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-leading-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/.

Wang, Echo and Paresh Dave. 2020. "Exclusive: Microsoft faces complex technical challenges in TikTok carveout." Reuters, August 10, 2020. Available at: https://www.reuters.com/article/idUSKCN256100/.

Whateley, Dan and Ashley Rodriguez. 2023. "New Lawsuit alleges TikTok owner let CCP access user data." *Business Insider*, May 15, 2023. Available at: https://www.businessinsider.com/new-lawsuit-alleges-tiktok-owner-let-ccp-access-user-data-2023-5#:~:text=ByteDance%20allowed%20a%20Chinese%20Communist,user%20data%2C%20the%20suit%20alleges.

Xinhua. 2013. "Xi Jinping: Tell China's story well and spread China's voice well." August 21, 2013. Available at: http://www.xinhuanet.com/zgjx/2013-08/21/c_132648439.htm

（新华社（2013）。〈习近平：讲好中国故事 传播好中国声音〉）

Xinhua. 2021. "Ministry of Foreign Affairs: Advises the U.S. to first investigate the situation in its own laboratories clearly." (August 24). Available at: http://www.xinhuanet.com/mrdx/2021-08/24/c_1310145019.htm（新华社（2021）。〈外交部：奉劝美方先把自家实验室情况调查清楚〉）

Xinhua. 2023. "Xi Jinping issues important instructions on cybersecurity and informatization work." July 15, 2023. Available at: http://www.news.cn/politics/leaders/2023-07/15/c_1129751651.htm. （新华社（2023）。〈习近平对网络安全和信息化工作作出重要指示〉）

Yang, Yingzhi and Brenda Goh. 2021. "Beijing took stake and board seat in key ByteDance domestic entity this year." Reuters, August 17, 2021. Available at: https://www.reuters.com/world/china/beijing-owns-stakes-bytedance-weibo-domestic-entities-records-show-2021-08-17/.

Zhang, Albert, Tilla Hoja, and Jasmine Latimore. 2023. "Gaming public opinion – *The CCP's increasingly sophisticated cyber-enabled influence operations.*" Australia Strategic Policy Institute, April 26, 2023. Available at: https://www.aspi.org.au/report/gaming-public-opinion.

Endnotes

1 The PRC framed various Western evidence-based allegations as "lies," including, the use of forced labour in Xinjiang, China's slowing economy, the severe impacts of Hong Kong's National Security Law on the city's freedom and democracy, etc.

2 The "Provisions on the Management of Algorithm Recommendations in Internet information Services" was implemented on March 01, 2022.

MLI
TRUE NORTH
IN CANADIAN PUBLIC POLICY

MACDONALD-LAURIER INSTITUTE

excellent

THOUGHT-PROVOKING

> Canada shall be the star towards which all men who love progress and freedom shall come.
>
> – Sir Wilfrid Laurier

high-quality

insightful

CONSTRUCTIVE

important

forward-thinking

Critically acclaimed, award-winning Institute

The **Macdonald-Laurier Institute** focuses on the full range of issues that fall under Ottawa's jurisdiction.

- Winner of the Sir Antony Fisher International Memorial Award (2011)
- Templeton Freedom Award for Special Achievement by a Young Institute (2012)
- Prospect Magazine Award for Best North America Social Think Tank (2018)
- Short-listed for the Templeton Freedom Award (2017)
- Cited by five present and former Canadian Prime Ministers, as well as by David Cameron, then British Prime Minister.
- *Hill Times* says **Brian Lee Crowley** is one of the 100 most influential people in Ottawa.
- *Wall Street Journal*, *Economist*, *Foreign Policy*, *Globe and Mail*, *National Post* and many other leading publications have quoted the Institute's work.

WHERE YOU'VE SEEN US

CTV

cpac FOR THE RECORD

Corus ENTERTAINMENT

CBC news

FP Foreign Policy

tvo

The Economist

WALL STREET JOURNAL

THE HILL TIMES

THE GLOBE AND MAIL
CANADA'S NATIONAL NEWSPAPER • FOUNDED 1844

NATIONAL POST

Ideas change the world

WHAT PEOPLE ARE SAYING ABOUT MLI

The Right Honourable Paul Martin

I want to congratulate the **Macdonald-Laurier Institute** for 10 years of excellent service to Canada. The Institute's commitment to public policy innovation has put them on the cutting edge of many of the country's most pressing policy debates. The Institute works in a persistent and constructive way to present new and insightful ideas about how to best achieve Canada's potential and to produce a better and more just country. Canada is better for the forward-thinking, research-based perspectives that the **Macdonald-Laurier Institute** brings to our most critical issues.

The Honourable Jody Wilson-Raybould

The **Macdonald-Laurier Institute** has been active in the field of Indigenous public policy, building a fine tradition of working with Indigenous organizations, promoting Indigenous thinkers and encouraging innovative, Indigenous-led solutions to the challenges of 21st century Canada. I congratulate **MLI** on its 10 productive and constructive years and look forward to continuing to learn more about the Institute's fine work in the field.

The Honourable Irwin Cotler

May I congratulate **MLI** for a decade of exemplary leadership on national and international issues. Through high-quality research and analysis, **MLI** has made a significant contribution to Canadian public discourse and policy development. With the global resurgence of authoritarianism and illiberal populism, such work is as timely as it is important. I wish you continued success in the years to come.

The Honourable Pierre Poilievre

The **Macdonald-Laurier Institute** has produced countless works of scholarship that solve today's problems with the wisdom of our political ancestors. If we listen to the **Institute**'s advice, we can fulfill Laurier's dream of a country where freedom is its nationality.

MACDONALD-LAURIER INSTITUTE

MLI
TRUE NORTH
IN CANADIAN PUBLIC POLICY

323 Chapel Street, Suite 300,
Ottawa, Ontario K1N 7Z2
613-482-8327 • info@macdonaldlaurier.ca

X @MLInstitute
facebook.com/MacdonaldLaurierInstitute
youtube.com/MLInstitute
linkedin.com/company/macdonald-laurier-institute