



ONLINE INFLUENCE AND HOSTILE NARRATIVES IN EASTERN ASIA

Published by the
NATO Strategic Communications
Centre of Excellence



ISBN: 978-9934-564-70-3

Author: Hannah Smith

Content Editor: George Steele

Project manager: Markku Mantila

Design: Kārlis Ulmanis

Thanks to: Nicholas Fang, Monika Gill, Benjamin Heap, Elina Lange, Rueban Manokara, Henrik Twetman, Kristina Van Sant, Thomas Uren, Elise Thomas, Katherine Mansted

Riga, April 2020

NATO STRATCOM COE

11b Kalciema Iela

Riga LV1048, Latvia

www.stratcomcoe.org

Facebook/[stratcomcoe](https://www.facebook.com/stratcomcoe)

Twitter: [@stratcomcoe](https://twitter.com/stratcomcoe)

This publication does not represent the opinions or policies of NATO or NATO StratCom COE.

© All rights reserved by the NATO StratCom COE. Reports may not be copied, reproduced, distributed or publicly displayed without reference to the NATO StratCom COE. The views expressed here do not represent the views of NATO.

Contents

EXECUTIVE SUMMARY	4
What are hostile information activities?	6
THE EAST ASIAN INFORMATION SPACE	8
Social media use in East Asia	11
HOSTILE INFORMATION OPERATIONS: CASE STUDIES	12
Hostile narratives in Taiwan.....	12
Activities related to the Hong Kong Protests	16
Information activities targeting Hong Kong	17
The campaign against Guo Wengui	20
The campaign against Gui Minhai	22
The campaign against NBA	22
Information activities in West Papua	26
Information activities in the Philippines	30
CONCLUSION	34
ENDNOTES	36

This report documents examples of hostile information activities that have originated in Eastern Asia and have been targeted at:

- Taiwan
- The Hong Kong-based protest movement
- West Papua
- The Philippines

Hostile information activities have been used to:

- shape international opinion,
- gain domestic political influence,
- affect the domestic politics and policymaking of another state,
- stifle dissent and discourage opposing views,
- and create justification for economic or diplomatic action by the hostile actor.

EXECUTIVE SUMMARY

Eastern Asia – which we will define as including East and Southeast Asia¹– is a region of increasing geopolitical competition with many racial, cultural and societal fractures. With the rapid expansion of inexpensive internet access, these fractures and tensions mean that many states in the region are both vulnerable to, and a source of, hostile information activities that are being used to achieve strategic goals both inside and outside the region.

This report documents examples of hostile information activities that have originated in Eastern Asia and have been targeted in the following countries:

- Taiwan
- The Hong Kong-based protest movement
- West Papua
- The Philippines

Historically, freedom of the press across much of East Asia has been severely restricted, with some governments looking to limit access to foreign media sources while simultaneously silencing domestic opposition.² Currently all 10 members of ASEAN are ranked in the bottom third of the Reporters Without Borders 2019 World Press Freedom Index.³ However, strict control over the flow of information is increasingly undercut by the popularity of new media and the creation of virtual communities. Nevertheless, recent changes in the way information is shared online, the use of sophisticated coercive surveillance tools, changes in how social media and citizens interact, as well as the rise of hostile information activities may alter how the internet affects societies and governments. In some environments, recreational internet use has been associated with more authoritarian world views.⁴

Because these activities often target social media, they have been difficult for law enforcement and national security organizations to police. Across the globe, countries are pursuing different methods of tackling the spread of hostile information activities with differing degrees of success. These approaches can range from law enforcement, temporary internet shutdowns, and attempts to legislate against ‘fake news’ or disinformation, through to wider societal media literacy initiatives.⁵

According to a 2017 Council of Europe Report, there are four criteria that are present in a successful information campaign: it provokes an emotional response, has a powerful visual component, has a strong narrative and is repeated.⁶ The early identification of all or some of these characteristics



can help detect campaigns that are more likely to be successful and inform attempts to counter them.

This paper describes a range of hostile information activities that attempt to reshape perceptions and influence events both domestically and externally. In countries such as the Philippines and Indonesia, online influence and disinformation is an industry that is used to manipulate domestic public discourse and to legitimize and support government actions such as the 'war on drugs'. However, hostile information activities are also used to shape how government actions are perceived externally. This can be seen in the various techniques that were used by the professional communications consultancy in Indonesia to shape the international perception of the West Papuan independence movement. Information activities have also been used to interfere in the internal politics of other nations. This is exemplified in the case study of Taiwan, where the Peoples Republic of China (PRC) used information activities to attack the opponents of the Chinese Communist Party (CCP) and justify diplomatic and economic retaliation to silence and repress dissenting views.

1. The persistent manipulation of the information space will not be solved with a single policy initiative or by social media companies alone. Rather, a robust suite of multifaceted responses is required, focusing on:
2. Fact-checking, digital literacy and critical thinking-based education
3. Measures to encourage a strong and independent media with the highest standards of journalistic integrity
4. Measures to encourage civil-society groups to research and transparently uncover hostile information activities
5. Steps to encourage social media companies to expand their capabilities to detect and remove hostile information activities.

Many social media companies appear to focus on tackling hostile information activities in their home markets first, for both political and competency-based reasons. Countries in Eastern Asia and other regions of the world, by contrast, have different cultural and linguistic backgrounds that make it more difficult for social media companies to understand and respond appropriately.



What are hostile information activities?

Information activities are activities designed to generate an effect in the Information Environment (IE). States employ information activities because they are inexpensive compared to other means of force interjection such as military influence, can be effective at achieving strategic goals, and are typically covert.⁷ As these activities often escape detection, the establishment of countermeasures is difficult, although non-state actors can also use information activities to achieve their strategic goals. This paper will focus on state-related activities.

These hostile information activities are inherently difficult to study in the contemporary IE, where social media and digital platforms are focal points, as hostile actors can easily obscure their identities, associations, and goals. When employed by hostile actors, information activities can consist of deceptive, disruptive, ill-intentioned communications, intended to distort information flows, undermine public debate, create artificial amplification of misleading narratives, intentionally distort facts, spread disinformation or oppress or promote a specific point of view.

Hostile information activities are often designed to establish, support or perpetuate specific narratives beneficial to a hostile actor. Narratives are the moral or deeper meaning that individuals draw from a specific story. They function as a shorthand that reduces complexity. Once a narrative is engrained in an audience it may serve as an organizing principle by which people make sense of new information and can powerfully influence what people believe.⁸ Hostile actors may seek to embed specific narratives through information activities. Analysing narratives associated with hostile information activities may allow the inference of strategic objectives of the hostile actor. Narratives promoted by hostile information activities are referred to below as hostile narratives.^[1]

Russia is the state currently most associated with hostile information activities, particularly its interference in the 2016 United States Presidential election, and multiple elections in the European Union.⁹ Several other states, including China¹⁰, Iran¹¹, Indonesia¹², and Bangladesh¹³, have also adopted similar methods to further their own strategic goals. Countries such as Australia, the United States, and the United Kingdom also employ information activities but regard them as occurring within the context of conventional military conflict.¹⁴

Actors engage in hostile information activities to gain or maintain the power to influence or control events that they view as strategically important. From the deployment of disinformation tactics used during the India-China Doklam border standoff¹⁵, nationalistic troll armies and 'doxing' tactics in use across Southeast Asia¹⁶, to sophisticated cyber-enabled influence activities in Taiwan, Hong Kong and on the Korean Peninsula, East Asia is ever-increasingly in the spotlight for the growing number and sophistication of these activities.

Within the past decade, the grassroots organizing power of social media has been displayed in anti-nuclear demonstrations in Japan¹⁷, Taiwan's 'Sunflower Movement'¹⁸, the pro-democracy protests in Hong Kong including the 2014 'Umbrella Movement'¹⁹ and the 2019 anti-extradition law protests²⁰, LGBTQAI community solidarity in Brunei after the Sultan implemented a new penal code²¹, and the 'upset election' in Malaysia which brought down the government of Najib Razak.²² Social media has also been used to mobilize hate crimes and internationally unlawful acts. As an example of this, the ethnic cleansing of Rohingya Muslims in Myanmar has been significantly supported by user posts on social media platforms such as Facebook.²³

This paper will document examples from the region where hostile information activities have been used to:

- shape international opinion,
- gain domestic political influence,
- affect the domestic politics and policymaking of another state,
- stifle dissent and discourage opposing views,
- and create justification for economic or diplomatic action by the hostile actor.

In all these examples, information activities contributed to the strategic objective of gaining or maintaining power in order to influence real-world events.

Interestingly, no country in East Asia has yet admitted to conducting hostile information activities. Many states in the region have legislation that attempts to tackle 'fake news', but few have strategies to respond to hostile information activities, with Singapore being a notable exception. This reticence to openly reveal strategies and responses could be attributed to the ASEAN norm of non-interference²⁴, the strong "Non-Alignment Movement" traditions of leading states like India and Indonesia, and the pervasive lack of trust of actors in the broader Indo Pacific region.

THE EAST ASIAN INFORMATION SPACE

The information space is the sum of the ways individuals learn about and are informed about their world. For an individual, personal experience shapes the way they receive and process information. However, (social) mass media is particularly influential because of its extensive reach and because it has become the way most people are informed about events that occur outside their immediate surroundings.



New methods of mass communication have previously disrupted the status quo in East Asia. Text messages were used to coordinate the revolutions that toppled Indonesian military leader General Suharto in 1998, as well as the ESDA II protests that forced the resignation of Philippines President Joseph Estrada in 2001²⁵. Additionally, anti-government bloggers in Malaysia first achieved some level of notoriety during the Reformasi (protest) of 1998 and the arrest of Anwar Ibrahim.²⁶ In 2007, Buddhist monks in Myanmar used Facebook to organize international support for the 'Saffron Revolution', resulting in the imposition of sanctions on members of the ruling military junta by the European Union, the United States, Canada, and Australia.²⁷

Although this is not the first time mass communication has been used to disrupt states, 'new media'²⁸ has increased the reach and speed of communications and made it

far easier to quickly spread hostile narratives. In East Asia, the continued improvement of telecommunications networks across the region was followed by an increase in the capability of multipurpose mobile devices, allowing users to communicate rapidly using photographs, recorded videos, text-based messaging, and social media. While this increased access to telecommunications technology has facilitated significant economic growth and access to information across the region, it has also created a new threat landscape for many states. For example, in September 2017 US military officials based in South Korea received a fake mobile text and social media messages advising US military personnel and their families to urgently evacuate the Korean Peninsula.²⁹



FOR WIDEST DISSEMINATION

**Eighth Army G2X
COUNTERINTELLIGENCE ADVISORY
as of 21 September 2017**

False NEO Evacuation Alerts

On Thursday, 21 September 2017, multiple reports indicated a fake NEO alert had been issued to multiple service members and spouses in the Republic of Korea.

USFK DID NOT ISSUE a "Real World Noncombatant Evacuation Operation Order". This false message has been delivered via Facebook and SMS messages.

What should you do?

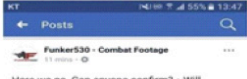
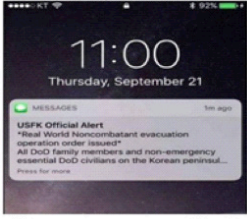
Always confirm NEO-related information with your NEO Warden.

Do not accept information from unconfirmed sources and verify official announcements with your appropriate chain of command.


Do not click any links or open any attachments included in unexpected correspondence. Verify the legitimacy of the sender.

If you received the alert depicted in this advisory or anything similar, please contact US Army Counterintelligence via the reporting hotlines listed to the right.

See something, say something!

Reporting Hotlines:
0503-323-3299
010-3100-0171



OPR: 8A G2X
FOR WIDEST DISSEMINATION
G2X-CIAR-26

Counterintelligence report warning of false NEO evacuation Alerts³⁰

Historically, freedom of the press in many East Asian states has been severely restricted, with some governments looking to limit access to foreign media sources while simultaneously silencing domestic opposition.³¹ Even as their economic and international diplomatic profiles have risen, all 10 members of ASEAN are ranked in the bottom third of the Reporters Without Borders 2019 World Press Freedom Index.³² However, strict control over the flow of information is increasingly undercut by the popularity of new media and the creation of virtual communities.

It was once predicted that the internet would promote democracy because it enabled better opportunities for political participation, education, and freedom of expression. This attractive hypothesis was supported by its initial research.³³ Recent developments, changes in information sharing, the use of sophisticated coercive surveillance tools,

changes in how social media and citizens interact, as well as the rise of hostile information activities may alter how the internet affects societies and governments.³⁴ Indeed, subsequent research has found that in some environments, recreational internet use was associated with more authoritarian world views.³⁵

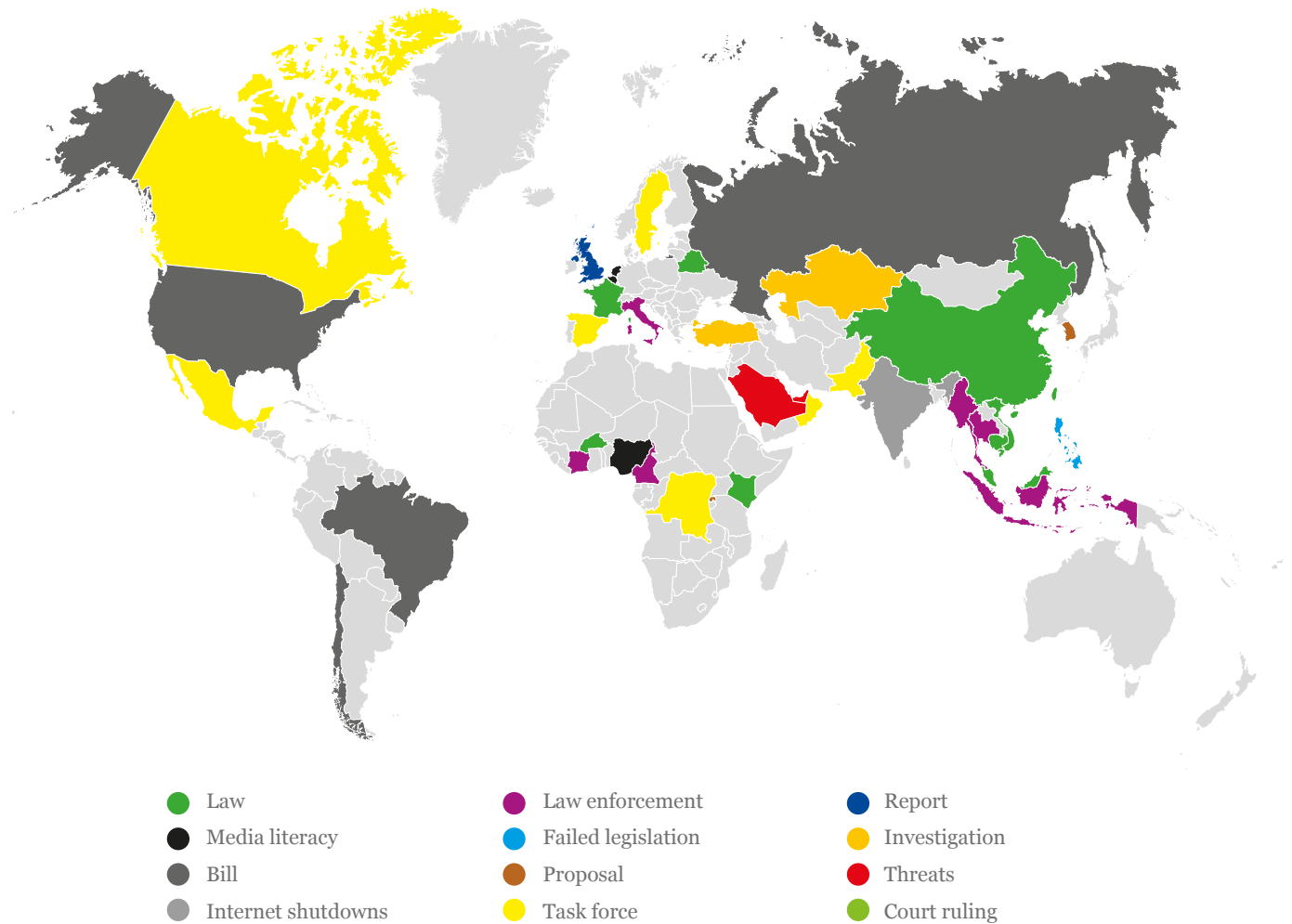
Social media platforms also appear to exacerbate hostile information activities. Social media revenues are driven by the amount of time that individuals use the platform, resulting in 'user engagement' becoming a key benchmark for social media companies. Unfortunately, engagement is increased by sensationalist and extreme content, so algorithm-driven platforms can lean towards the promotion of extreme views by delivering them broadly to their users.³⁶ Individual users are also not passive consumers. They engage in 'participatory



propaganda' where they adapt and amplify hostile narratives.³⁷

Because these activities often target social media, they have been difficult for law enforcement and national security organizations to police. This has effectively lowered the threshold at which one nation—including those with weaker militarily

capabilities—can affect the affairs of another. Across the globe, countries are pursuing different methods of tackling the spread of hostile information activities with differing degrees of success. These approaches can range from law enforcement, temporary internet shutdowns, and attempts to legislate against 'fake news' or disinformation, through to wider societal media literacy initiatives.



Map from Poynter displaying different state actions to stem disinformation and misinformation³⁸



Social media use in East Asia

For those with access, social media usage in East Asia is typically high, although there are considerable regional differences. Internet penetration in Southeast Asia, which has a significant overlap with East Asia, is at 63 percent³⁹, with social media penetration at 61 percent, an increase of 6 percent from 2018⁴⁰. Internet users in Southeast Asia are also among the most engaged globally.

Currently, users in the Philippines spend an average of 10 hours and 2 minutes using the internet daily, with 4 hours and 12 minutes of that time spent on social media.⁴¹ At the other end of the spectrum, users in Japan, long considered one of the most technologically advanced countries in the world, spend only 3 hours and 45 minutes using the internet and 36 minutes a day on social media.⁴² Typically, time on both the internet and in social media across the region of East Asia is closer to the

experience of users in the Philippines, than to the users in Japan.⁴³

The lower internet penetration, compared to markets in Western Europe and North America, and a consistent rise in new users, is attractive to current and emerging social media platforms looking to continue their meteoric growth. Technological innovations that both expand internet access and reduce the cost of 'smart' devices are likely to continue this rapid increase in digital connectivity. Internet platform companies actively attempt to accelerate this trend. Facebook, for example, provides its service free to the subscribers of local telecommunications providers via its Free Basics program in targeted countries⁴⁴ and Alphabet's Project Loon is attempting to deliver internet access to rural and remote areas via high-altitude balloons.⁴⁵

Country	China ⁴⁶	Indonesia ⁴⁷	Philippines ⁴⁸	Taiwan ⁴⁹
Internet Users and Penetration	802 m, 57%	150 m, 56%	76 m, 71%	20.8 m, 88%
Active Social Media Users and Penetration	1.007 bn, 71%	150 m, 56%	76 m, 71%	21 m, 89%
Daily internet use (hours, minutes)	5h 52m	8h 36m	10h 2m	7h 39m
Top 5 Social Media Platforms	WeChat (79%), Baidu Tieba (72%), QQ (68%), Sina Weibo (60%), YouKu (59%)	YouTube (88%), WhatsApp (83%), Facebook (81%), Instagram (80%), Line (59%)	Facebook (97%), YouTube (96%), FB Messenger (89%), Instagram (64%), Twitter (54%)	YouTube (90%), Facebook (89%), Line (84%), FB Messenger (57%), Instagram (49%)

Table 1: Internet and social media statistics for selected countries in eastern Asia⁵⁰



HOSTILE INFORMATION OPERATIONS: CASE STUDIES

Hostile narratives in Taiwan

In Taiwan, the CCP, uses a variety of disinformation tactics and techniques in what it considers to be a renegade province, unconstrained by concerns about interfering in the affairs of another state.⁵¹

The CCP uses a “three warfares” strategy that uses public opinion warfare (舆论战), psychological warfare (心理战), and legal warfare (法律战) “to control the prevailing discourse and influence perceptions in a way that advances China’s interests while compromising the capability of opponents to respond.”⁵² The PRC harnesses these narratives to support and justify its actions. In the South China Sea, for example, the PRC uses narratives of historical possession to claim sovereignty over disputed territory.⁵³ With regards to Taiwan, the narrative the PRC uses internationally is that it seeks the ‘reunification of China’, without acknowledging that “Taiwan has never been a part of the People’s Republic”⁵⁴. Within Taiwan, the PRC uses sophisticated public disinformation campaigns targeting Taiwanese domestic politics and uses technology to falsely amplify narratives that support Beijing’s interests (as seen in the harnessing of groups of state-backed internet commenters and bot networks).⁵⁵

A 2019 report from the Digital Society Project listed Taiwan alongside Latvia as being most affected by foreign governments’ dissemination of false information, with the actions described as occurring extremely often in all key political issues.⁵⁶ However, while across the region cyber-enabled influence activities are often overt social media campaigns, in Taiwan they also leverage more traditional espionage activities, forming sophisticated online campaigns. For example, in early 2018 the Taipei District Prosecutor’s Office uncovered a multi-year operation run by the CCP that aimed to infiltrate the Taiwanese military.⁵⁷ This operation used traditional intelligence collection methods to inform more targeted cyber-enabled influence activities across websites and social media networks to target Taiwan’s military and its domestic networks.⁵⁸

Alongside the use of traditional media, the CCP has incorporated the use of microblogging sites, social media, messaging apps, and content farms to produce and further disseminate disinformation throughout Taiwan.⁵⁹



泛藍社群中，那些痛批蘇政府的文章，多半都能引發高度迴響。其中雖然不乏聯合新聞網、中時電子報等主流媒體的內容，然而卻有不少文章竟是專向蓄意更改標題、賣弄眼球的「內容農場」網站，同樣引發熱烈迴響，致使泛藍社群反倒淪為有心人士操弄對立情緒，大賺流量的「金礦」。

資料來源：今周刊《看不見的黑手？泛藍社群遭「內容農場」攻陷》、維基百科《內容農場》

“注意，這些是假新聞的網站！”

▶ 什麼是內容農場？

透過合法、非法手段製造大量品質低劣、不具參考性的新聞，透過聳動的標題吸引讀者點閱，以賺取點閱率和網路流量為目的。

▶ 哪些網站是內容農場/假新聞？

- aboutfighter.com (奮鬥者)
- bldaily.com (美麗日報)
- Bomb01.com
- BuzzHand
- cocohk系列
- cocomy.net (COCO大馬)
- damaday.com (大馬加油)
- ezp93.com
- funnyanecdote.com (新政聞)
- foyuanvip.com (佛道)
- gigacircle.com
- happytifyhome (笑趣聞)
- happtify.cc (歡享網)
- hotstartabloid.com (STAR星聞)
- imama.tw (媽媽)
- kknews.cc (每日頭條)
- ptt01.cc (PTT01 娛樂新聞)
- read01.com (壹讀)
- teepr.com (趣味新聞)
- twgreatdaily.com
- www.contw.co

Image of suspected Chinese-linked content farms.⁶⁰

As noted by Chen and Cole, disinformation campaigns aimed at Taiwan have slowly become more refined, with “reports of CCP backed groups hiring Taiwanese linguists to create posts for various social media pages and content farms.”⁶¹ The authors argue that by doing so, “agents of disinformation have gradually removed linguistic idiosyncrasies (e.g., use of simplified Chinese, local terms, etc)”. This has in the past been an identifying factor in recognizing foreign generated disinformation in Taiwan.⁶²

As cross-straits tension increases, Taiwan has also become a testing ground for many emerging PRC information warfare tactics aimed at shaping the political landscape. For example, during the regional elections in 2018, the rapid popularity and election of the Kuomintang (KMT) candidate Han Kuo-yu, in what was formerly considered a Democratic People’s Party (DPP) safe seat, raised the suspicions of CCP interference in the election. While Han quickly became one of the most popular candidates, with his official Facebook

page gathering more than 500,000 followers⁶³, an investigative report from Foreign Policy indicated that a large portion of his initial popularity was manufactured by proxies for the PRC.⁶⁴ These proxies established fan pages on social media, followed by numerous fake accounts, giving the impression of legitimate online engagement. This also highlights the use of avalanche tactics – the process of manufacturing false levels of engagement initially – which then becomes popularized and initiates real engagement, thus generating support for preferred candidates or policies.

The largest of these social media pages, *‘Han Kuo-yu Fans for Victory! Holding up a Blue Sky!’*, was created the day after Han announced his candidacy, and is alleged to have produced and distributed disinformation, which was then shared to other social media sites. Following his social media and electoral success, Han has gone on to become the preferred PRC presidential candidate.





Facebook fan page for 'Han Kuo-yu Fans for Victory! Holding up a Blue Sky!', created the day after Han announced his candidacy.

Due to high penetration and interconnections to digital platforms in Taiwan, social media has played a significant role in the successful spread of hostile narratives. In particular, bulletin board (messaging) systems and encrypted messaging apps play a significant role in the spread of disinformation, with hostile narratives leveraging real social sentiment and aiming to amplify those messages on these platforms.⁶⁵

The most popular of these messaging apps, LINE, is used to share information within closed groups. This creates a particular challenge in counteracting disinformation as the content shared within these closed

groups is difficult to track and the information is spread by what are often known and trusted sources.

Another challenging source of disinformation is "PTT", an open-source bulletin board with more than 1.5 million registered users, who collectively post more than 500,000 comments daily.⁶⁷ The platform hosts a large number of pro-unification pages and is considered to be a significant source of disinformation.⁶⁸ There have also been accusations against journalists of monitoring the platform for breaking news and publishing content with little fact-checking, further amplifying and legitimizing disinformation.⁶⁹





A photo falsely claiming Taiwanese pineapples were being secretly dumped circulated on the private messaging app LINE.⁶⁶



A doctored image of DPP candidate, Chen Chi-ai, shared on PTT and later on mainstream media, alleging him wearing of an earpiece to cheat during a live debate with rival Han Kuo-yu.⁷⁰

The Main Narratives

Three main narratives that have emerged from disinformation in Taiwan:

- (a) the inevitability of reunification;
- (b) the cost of separation;
- (c) narratives designed to weaken democracy and make the Taiwanese Government appear weak; this includes sub-narratives specifically designed to:
 - (i) narratives to support certain candidates perceived as favoring Beijing's interest, and/or;
 - (ii) narratives to undermine certain candidates, perceived as being less aligned with Beijing's interest.

Most importantly, this inundation of hostile narratives in Taiwanese political discourse can exacerbate underlying tensions and weaken trust within democratic institutions. In response to these growing concerns, there has been a push by both the Taiwanese

government and the private sector for greater media literacy.⁷¹ This has been coupled with the promotion of fact-checking resources that aim to flag false claims online and provide additional context to readers.⁷²

Fact-checking resources, however, are not immune to disinformation. Crowdsourced collective knowledge databases such as Wikipedia, for example, have become the battlegrounds for hostile information activities.⁷³

In October 2019, a BBC investigation found 1,600 edits across 22 Wikipedia articles that were deemed politically sensitive to the PRC.⁷⁴ While the investigation could not attribute the origin of the edits or why they occurred, the systematic editing reflects a widespread practice of altering collective knowledge databases to support a desired narrative.



Issues with the widespread editing of information in open-source repositories are not limited to the databases themselves. Internet-connected smart speakers, including Amazon's Alexa, Google's Home, and Apple's HomePod, often draw on these sources to inform virtual assistants. This particular

vulnerability was highlighted in early September 2019 when a number of virtual assistants' response to the question 'What is Taiwan?' changed from "a state in East Asia" to "a province of the PRC" multiple times in the course of a single day.⁷⁵

Activities related to the Hong Kong Protests

On 19 August 2019, Twitter released data on accounts that it had identified as being involved in a hostile information activity directed against the "anti-Extradition Law Amendment Bill" (anti-ELAB) protest movement in Hong Kong.⁷⁶ Facebook also dismantled a smaller information network operating on its platform.⁷⁷

Twitter and Facebook linked this hostile information activity to the Chinese government. Twitter stated that "some accounts accessed Twitter from specifically unblocked IP addresses originating in mainland China" and Facebook stated that although "the people behind this activity attempted to conceal their identities, our investigation found links to individuals associated with the Chinese government." The data and methodology that Facebook and Twitter used to link these operations to the PRC have not been made public and we have not independently verified their assertion that this activity is linked to the Chinese government. Twitter states "we employ a range of open-source and

proprietary signals and tools to identify when attempted coordinated manipulation may be taking place, as well as the actors responsible for it".⁷⁸

Both Facebook and Twitter have access to data that they had not made available earlier that could be used to link this activity to the PRC. Beyond the mainland IP addresses mentioned by Twitter, this would include account information such as phone numbers and email addresses used in account sign-up procedures, and information about the computing environment these accounts used to access Twitter or Facebook, operating system version, browser version and plugins, graphics configuration, as well as presence of other social media accounts.⁷⁹ In a large network of accounts, this information could be analyzed and combined with open source investigation to identify possible links to the PRC government.

Assuming the linkage of this operation to the PRC is correct, the identification of this activity is significant because it would be



the first confirmed case where the PRC has systematically manipulated social media to target external audiences outside of Taiwan. This example of hostile information activity is based upon original Australian Strategic Policy Institute (ASPI) research analyzing the dataset released by Twitter and has previously been published in 'Tweeting through the Great Firewall'.⁸⁰

In addition to the operation attacking the Hong Kong protests, analysis of the data released by Twitter identified at least four prior information activities targeting political opponents of the CCP.⁸¹ Although we cannot confirm the contribution of the PRC government, we can confirm that the behavior in the data set is consistent with their interests.

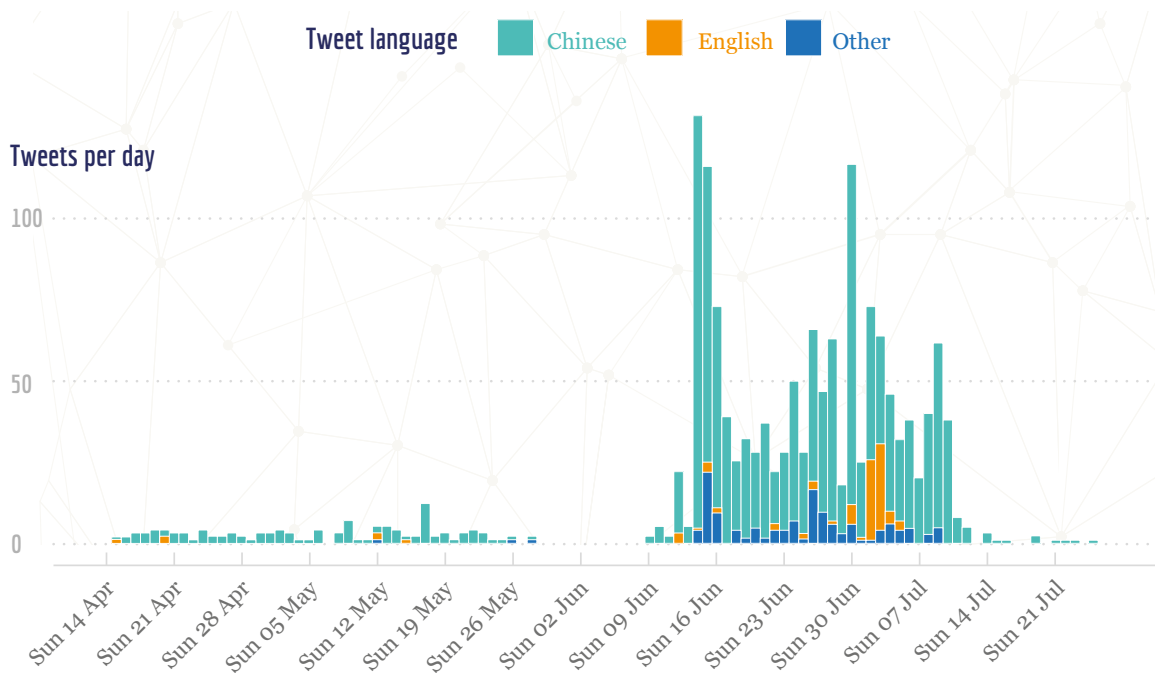
Information activities targeting Hong Kong

China's domestic internet is structured by technocratic control managed by the Cyberspace Administration of China⁸² and devolved content regulation by government entities, industry and Chinese "netizens"⁸³. Recent research suggests that the Chinese government pays for as many as 448 million inauthentic social media posts and comments a year⁸⁴, with the aim of distracting the population from social mobilization or protest actions.

The first PRC-linked content related to the 2019 anti-ELAB protests that ASPI research

identified appeared on 14 April 2019, when the account @HKpoliticalnew (profile description: Love Hong Kong, love China. We should pay attention to current policies and people's livelihood. 愛港、愛國，關注時政、民生) tweeted about the planned amendments to the extradition bill. In the dataset released by Twitter Hong Kong-related, tweets were infrequent but steadily increased over April and May until a significant spike on 14 June⁸⁵, when over a million Hong Kongers marched in protest against the extradition bill.⁸⁶





(Hong Kong related tweets per day from 14 April 2019 to 25 July 2019.)

Significant days in the anti-ELAB protests match significant spikes in Twitter activity. A major spike is seen on 1 July when protestors stormed the Legislative Council building. 1 July also marks the beginning of English-

language tweets, presumably in response to the growing international interest in the Hong Kong protests. In this dataset tweets related to Hong Kong gradually decline before ending on 25 July.⁸⁷

The Main Narratives

Three main narratives emerge from the tweets targeting the Hong Kong protests:

- Condemning the protestors by framing them as destructive rioters;
- Support of the Hong Kong police and 'the rule of law';
- Conspiracy theories about Western involvement in these protests.



Condemning the protestors:



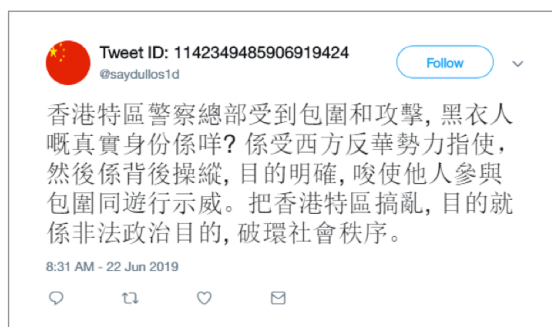
Translation: '#HongKong #HK #HongKong #FugitiveOffendersOrdinance #Protests The old Chinese saying put it well: 'Judge a person by their words, as well as their actions'. Take a look at those in the opposition parties and the Hong Kong independence extremists. Apart from instigating street demonstrations, violent attacks, assaulting police officers and disturbing the social order in Hong Kong, they have done nothing that is actually advantageous to the development of Hong Kong. This abnormal fetus of a "freak demonstration" that the opposition parties and Hong Kong independence people gave birth to is becoming more violent as it heads down this evil road'.⁸⁸

Support for 'rule of law':



Translation: 'The amendment to the Fugitive Offenders Ordinance will only make Hong Kong's legal system more complete. After all, the law is the cornerstone of safeguarding fairness and justice in society. We can't allow loopholes in the legal system to allow criminals to escape the arm of the law'.⁸⁹

Conspiracy theories:



Translation: 'The Hong Kong SAR police headquarters were surrounded and attacked. Who were the people wearing black? They were acting under the direction of western anti-China forces. They're manipulating things behind the scenes, with a clear purpose to instigate others to participate in the demonstration and the encirclement. They're bringing chaos to Hong Kong SAR with an illegal political goal and disrupting the social order'.

This tweet was written in traditional Chinese characters and switches between Standard Chinese and Cantonese, suggesting that the author was a native mandarin speaker but their target audience was Cantonese speakers in Hong Kong.⁹⁰



The campaign against Guo Wengui

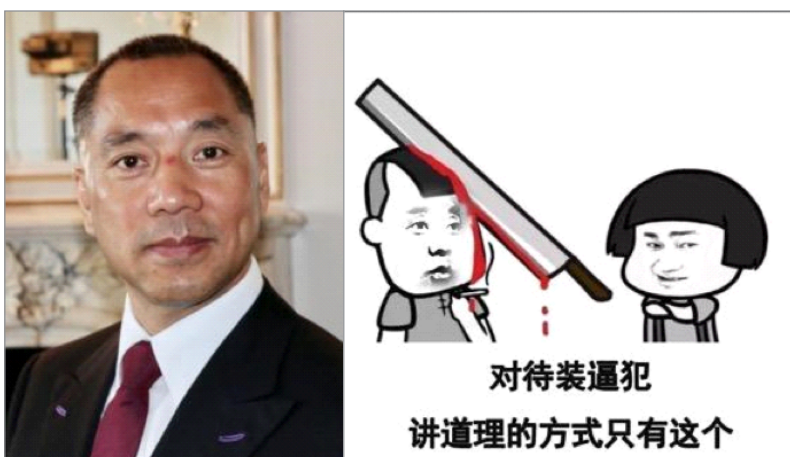
The earliest activity ASPI identified that aligned with CCP interests was directed against Guo Wengui, an exiled Chinese businessman who is now living in the United States. This was the most extensive information activity in the Twitter dataset and is considerably larger than the activity directed against the anti-ELAB Hong Kong protests.⁹¹

Guo, also known as Miles Kwok, has used Twitter and YouTube to publicize allegations of corruption against senior members of the Chinese government⁹², and is believed to have fled to the United States in 2015 around the time an associate, former Ministry of State

Security vice minister was arrested.⁹³

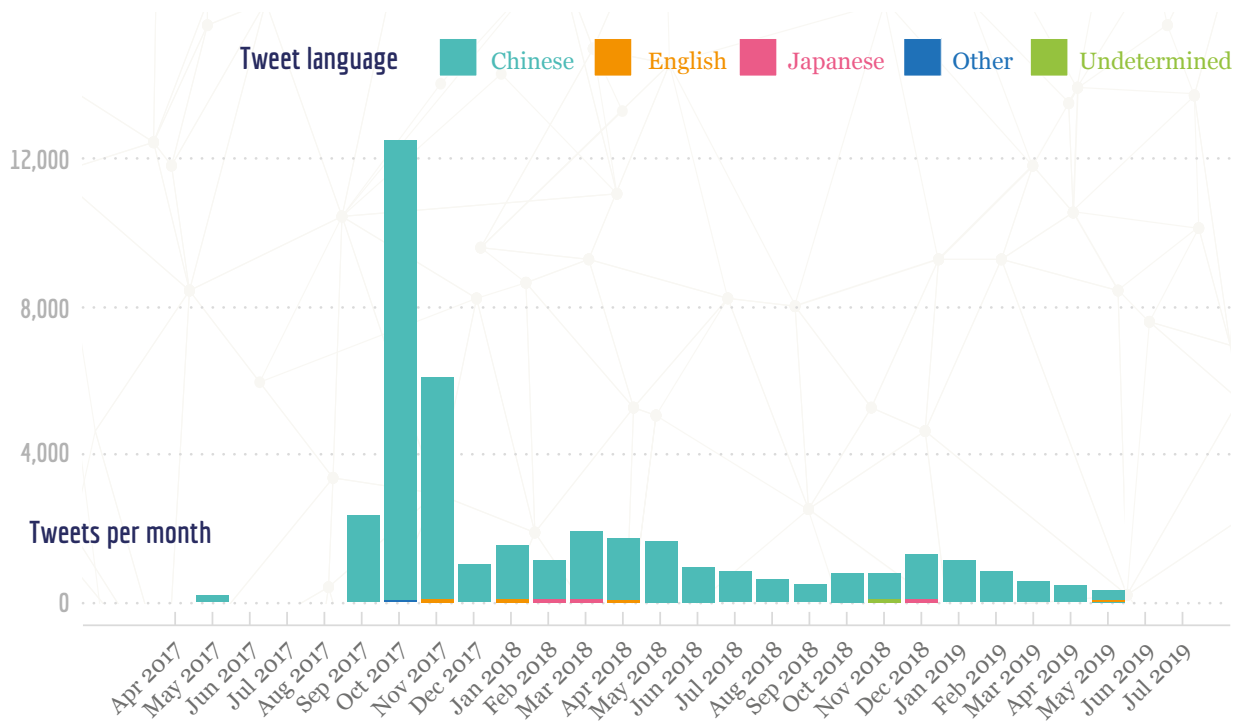
The Chinese government has, in turn, accused Guo of corruption and has had Interpol issue an international arrest warrant, or 'red notice', seeking his arrest and return to China.⁹⁴ Guo has become a vocal opponent of the Chinese government⁹⁵, despite having himself been accused of spying on their behalf in July 2019.⁹⁶

Within the Twitter Hong Kong dataset, the hostile information activity targeting Guo began on 24 April 2017, five days after the Interpol red notice was issued, and continued until the end of July 2019.⁹⁷



(Guo Wengui, and an image from a tweet threatening violence against him.)





(Tweets per month in the information operation targeting Guo from 2017 to the end of the dataset in July 2019.)

ASPI research has identified at least 38,732 tweets from 618 accounts in the dataset which directly targeted Guo. These tweets are largely attacks on his character including

personal criticism, accusations of criminality, accusations of treason, and criticisms of his relationship with the controversial US political figure Steve Bannon.⁹⁸



The campaign against Gui Minhai

Another information activity within the Twitter dataset targeted Gui Minhai, a Chinese-born Swedish citizen. Gui is one of a number of Hong Kong-based publishers specializing in books about China's political elite who disappeared under mysterious circumstances in 2015.⁹⁹ Gui was found to have been subsequently taken into Chinese police custody for his role in a fatal 2003 traffic accident in which a schoolgirl was killed. Gui has been in and out of detention since 2015 and has made a number of televised confessions¹⁰⁰ which many human rights advocates believe to have been coerced by the Chinese government.¹⁰¹

The Twitter campaign targeted against Gui Minhai is entirely in Mandarin, presumably because the target audience is overseas Chinese. The tweets emphasize Gui's role in the traffic accident, painting him as a coward for attempting to leave the country and blaming Western media for interference in the Chinese criminal justice process.¹⁰²

Additional campaigns were identified within the Twitter dataset that targeted Yu Wensheng, a human rights lawyer and prominent CCP critic, and PLA veterans that were protesting to demand unpaid retirement benefits.¹⁰³

The campaign against NBA

The recent controversy over a tweet by the General Manager of the National Basketball Association's (NBA) Houston Rockets team illustrates the way narratives can be combined with economic power to achieve effects.

The NBA is a USD 8 billion revenue global sports business¹⁰⁴, with an annual PRC direct revenue estimated at USD 500 million¹⁰⁵ growing at double-digit percentages¹⁰⁶, which also allows the players to receive significant individual endorsement income. The NBA is also the most followed sports league in the PRC.¹⁰⁷

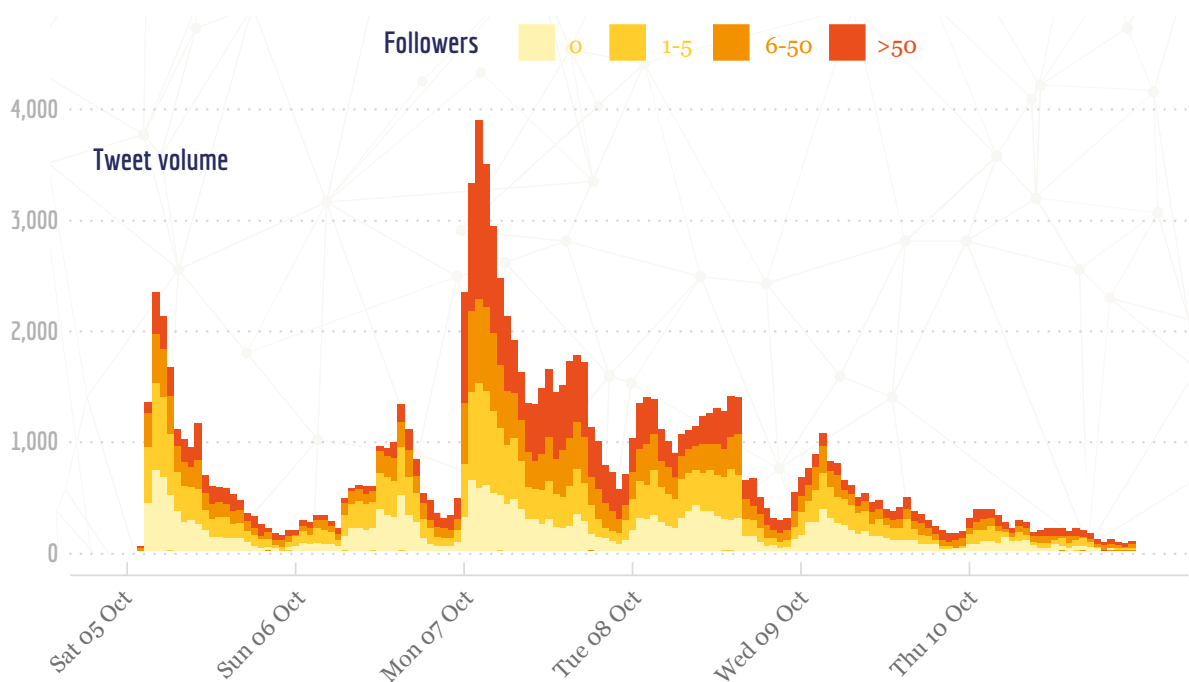


Image of suspected Chinese-linked content farms.¹⁰⁸



On October 4, the General Manager of the Houston Rockets, Daryl Morey, tweeted in support of the Hong Kong protests. Despite Twitter being actively blocked in the PRC, within minutes Morey was deluged with tweets in response—more than 16,000 within 12 hours.¹⁰⁹ An analysis published in the Wall Street Journal examined 168,907 tweets directed at Morey between 4 and 10 October 2019 captured by Clemson University researchers Darren Linvill and Patrick Warren. ASPI researchers have independently verified the major findings of this analysis, although the data collection methods and timing differed, as did the exact numbers of tweets examined.

This hostile information activity was not contained within the dataset released by Twitter, but analysis of the tweets directed against Daryl Morey had the characteristics of a co-ordinated state-backed operation. The accounts had relatively few followers and many had never tweeted before replying to Morey.¹¹⁰ The figure below, comprised of the independent ASPI research shows that most of the tweets directed to Daryl Morey came from accounts with few followers.

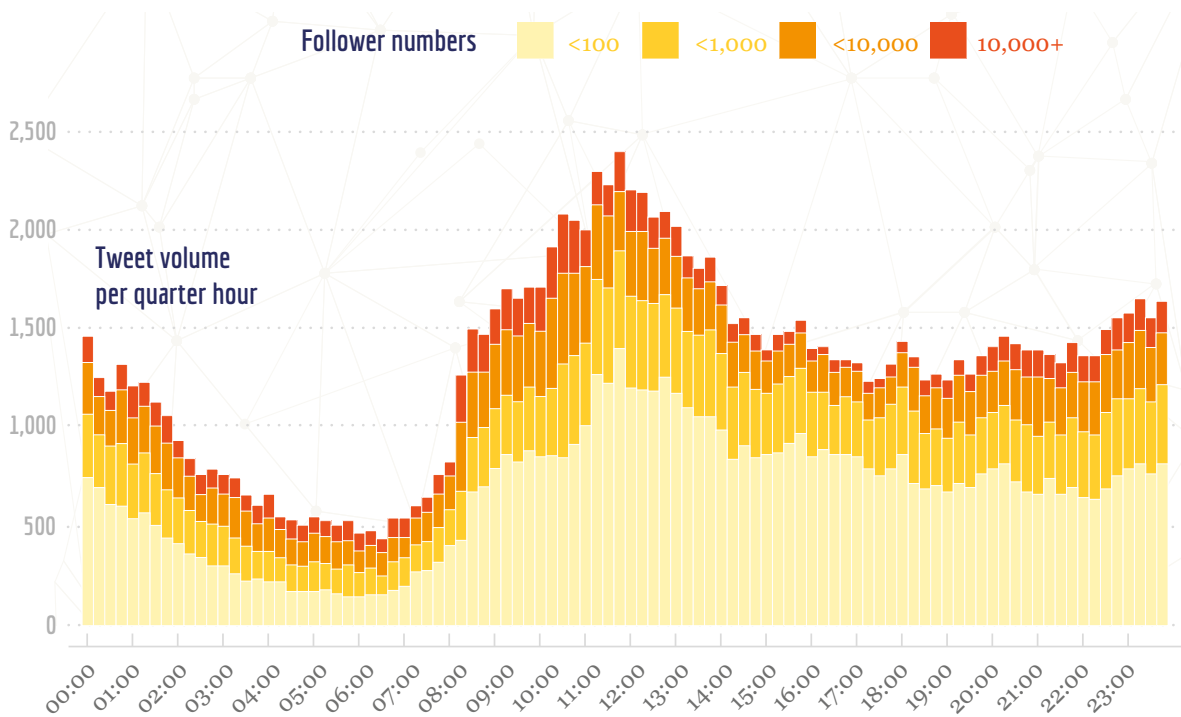


Tweets per hour by follower count.



The presence of large numbers of authentic Twitter users is also inconsistent with the PRC's attempts to ban and block Twitter access within mainland PRC, and its attempts to repress, detain and silence domestic

Twitter users.¹¹¹ The figure above shows the volume of tweets directed to Daryl Morey relative to Beijing time. The pattern of tweets is consistent with account holders operating in Beijing time.

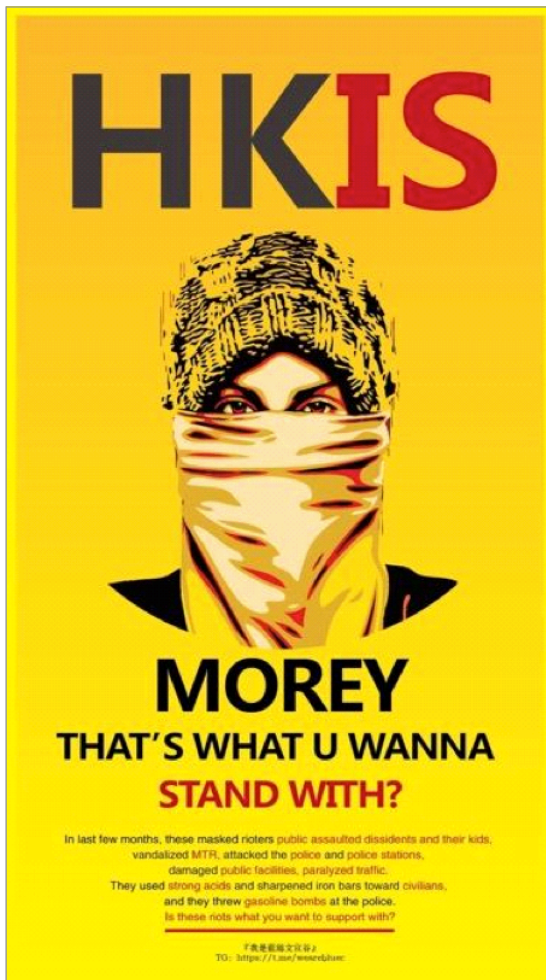


Tweets per quarter-hour by account follower numbers.

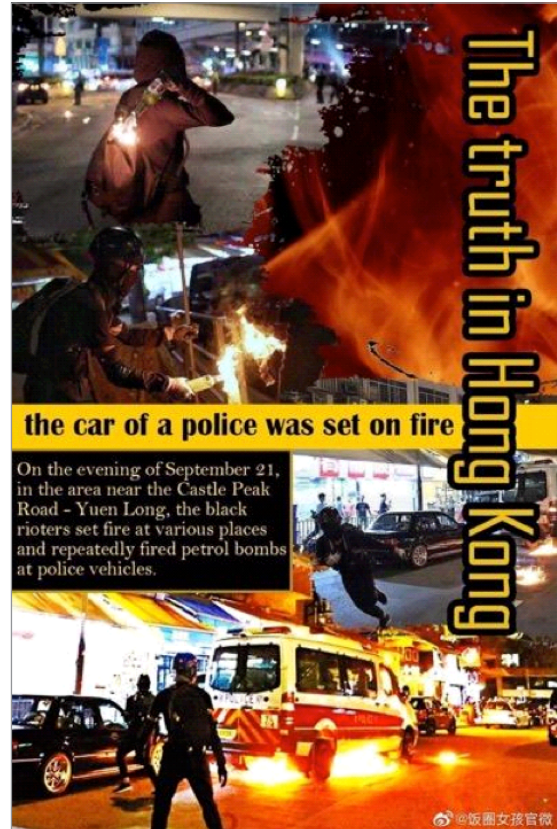
Many of the tweets directed at Morey contained the abbreviation "NMSL", an acronym for 'your mother is dead' or 你妈死了 and were clearly designed to intimidate.

Some of the tweets also reflected the major narratives of the information operation targeting the Hong Kong protests.





This image addressed directly to Daryl Morey on Twitter uses themes that match those used in the state-backed campaign targeting the Hong Kong protests.



Another image addressed directly to Daryl Morey on Twitter that matches the narratives employed in the state-backed hostile information activity directed against the 2019 Hong Kong Protest movement.

This twitter barrage was quickly followed by a full-court press of other tactics designed to silence criticism of the PRC. The multi-modal nature of these narratives demonstrate that state-backed hostile information activities are rarely 'one-off' reactive incidents, but instead, have a level of coordination and are serving broader strategic objectives related to shaping and constraining the flow

of information in order to advance the state actor's interests.

China Central Television (CCTV) suspended television broadcasts and Tencent, the Chinese Internet-based platform company, suspended live streaming of NBA preseason games.¹¹² The Chinese Basketball Association suspended cooperation with the Houston



Rockets¹¹³, and all official Chinese NBA partners suspended their ties with the league.¹¹⁴ The PRC's Consulate-General in Houston lodged an official protest¹¹⁵, and The Global Times, an English-language state media organization, stated that Morey's tweet had "set the team's Chinese fans ablaze", that he should "respect the feelings of Chinese fans" and "warned global brands that "entities

that value commercial interests must make their members speak cautiously".¹¹⁶

In this example, an information activity was used to justify further economic action to reinforce self-censorship in the NBA relating especially to the Hong Kong protests, but also other potential issues deemed sensitive by the Chinese Communist Party.

Information activities in West Papua

Online misinformation and disinformation have rapidly become endemic in the political life of Indonesia. Online influence and disinformation campaigns were allegedly used by both sides in the 2019 presidential elections.¹¹⁷ An entire cottage industry, known as "buzzers", has sprung up to service the demand for positive promotion and disinformation alike. The Indonesian police have broken up "fake news factories"¹¹⁸ which have allegedly played influential roles in swaying elections and sparking political protests.¹¹⁹

Spreading disinformation (often referred to as "hoaxes" in Indonesia) is illegal under the controversial "Information and Electronic Transactions Act", but experts suggest that in practice arrests and prosecutions are highly politicized. Analysis has found that during the 2019 presidential elections, punishment was dealt out almost exclusively to those spreading disinformation that attacked the government and president and not to those

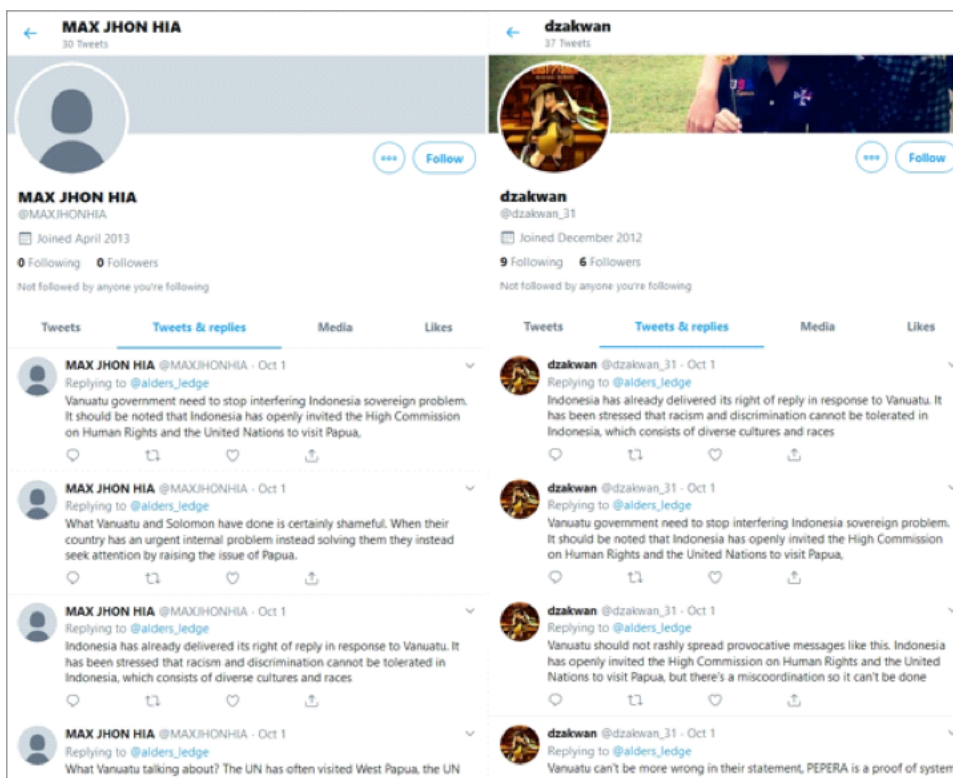
which were undermining their opponents.¹²⁰ For example, in the wake of the elections, protests broke out in Jakarta against the victory of incumbent President Joko Widodo. In response, the government-imposed restrictions on social media, a move which it claimed was necessary to stop the spread of hoaxes which it blamed for inflaming tensions.¹²¹

However, these organized campaigns extend far beyond election cycles and often beyond Indonesia's borders. Recent joint ASPI-Bellingcat research has uncovered overlapping disinformation campaigns aimed at shaping the international perception of the Indonesian government's actions in West Papua.¹²² These campaigns that appear to be designed to shape external perceptions of domestic actions were conducted primarily in English, operated across multiple platforms, and spread content which supported a pro-government narrative and undermined the independence movement in West Papua.



In addition to creating and promoting content, one of the campaigns also engaged in targeted harassment of journalists, independence leaders, and foreign politicians on social media. The likely goal was to reduce

the risk of censure from the international community over Indonesia's actions in West Papua as well as to influence the policies of foreign governments and international bodies such as the United Nations.

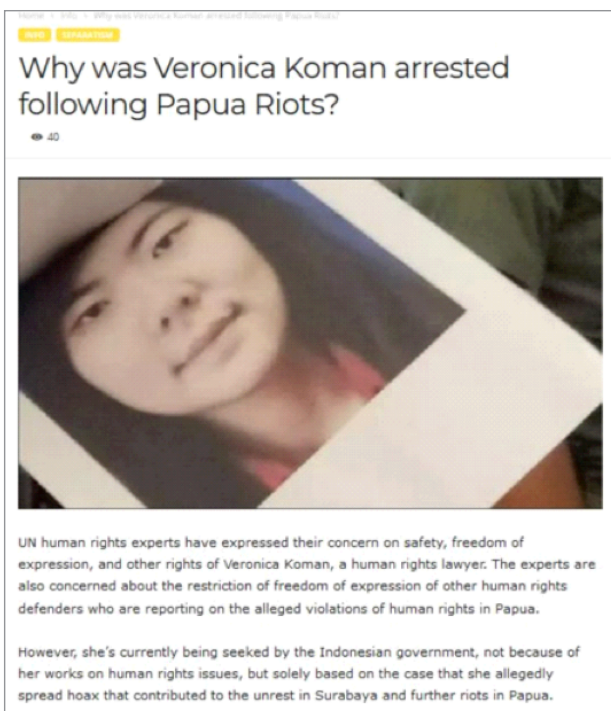


A screenshot showing inauthentic accounts harassing Twitter user @alders_ledge.

The existence of multiple seemingly independent campaigns using similar tools and methods to achieve similar goals on the same issue is a reflection of the increasingly crowded narrative battlespace online. Information activities are no longer an exceptional measure in this space. Instead, they are an increasingly normalized aspect of international and even domestic conflicts.

The larger of the two campaigns analyzed in the recently released research exemplifies the professionalization of the disinformation industry in Indonesia. Open-source analysis, later confirmed by Facebook, traced the campaign to a professional communications consultancy called InsightID. InsightID employed a team of content writers, Facebook ad specialists, and developers,





A screenshot of a "news" article on infowestpapua.com defaming Veronica Koman, a human rights lawyer who has been targeted by the Indonesian government.

and appears to have had several legitimate marketing clients in addition to its work in West Papua.

InsightID's West Papua operation was based around "brands": websites and social media accounts branded with the same names and logos and promoting the same content, in much the same way that a legitimate news organization would have a website and social media accounts bearing its name and logo. InsightID also created significant amounts of content, including "news" articles,

infographics and videos, to convey pro-Indonesian government narratives and attack the pro-independence forces, in particular, the United Liberation Movement for West Papua and its leader, Benny Wenda. It also included content attacking international media for its coverage of violence perpetrated by the Indonesian security forces in West Papua. Some of this information was factually true but was slanted to present the Indonesian government in a favorable light while some of the content was outright false.



The content was first hosted on the branded domains, and then shared, tweeted and amplified across the brand's social media accounts. Methods of amplification were adapted for each platform. Search engine optimization techniques were used to boost the ranking of the branded domains in organic search results on Google. On Facebook, paid advertisements were used to target Facebook users in Europe and the United States. On Twitter, fake accounts were used to retweet, "like" and comment on the branded accounts' tweets. Twitter and Facebook accounts were used to share Youtube videos. There is also some indication that content may have been promoted on Whatsapp.

Almost all of the Twitter accounts made some use of hashtags, and the amplifier accounts on Twitter often tagged key individuals in their tweets (branded accounts usually did not). An interesting twist was that in addition to using very broad hashtags (such as #westpapua) the accounts also sometimes targeted "opposition" hashtags (such as #westpapuafreedom). There were two likely goals for this practice: firstly, to spread a misleading message to those seeking more information about the independence movement, and secondly to simply flood pro-independence hashtags with anti-independence content as a form of 'reverse censorship' attempted to drown out opposing legitimate voices.

Other related tactics employed on Twitter included 'typo-squatting'. This is creating a name that has only a one or two characters different from an opponent's. For example, the Twitter account @WestPapuaMedia is a well-established pro-independence account. InsightID registered the account @WestPapuaMedia and filled it with anti-independence content. Another example of impersonation was the "West Papua Freedom" brand (which operated on Twitter under @WestPapuaFreed and after that account was banned, @WestPapuaFreed2). This brand positioned and styled itself as a pro-independence account, but the content was pro-Indonesian government and anti-independence.

There is no available research into how effective this campaign may have been in swaying domestic or international opinion. From Facebook's blog¹²³, we know that hundreds of thousands of Facebook and Instagram accounts followed at least one of the InsightID accounts, and it can be conservatively estimated that tens, and likely hundreds, of thousands of Twitter of users, also saw at least some of the content. Beyond the immediate context of West Papua, the key significance of this case study is that it demonstrates the way in which hostile information operations are coming to play in domestic conflicts.



Information activities in the Philippines

In a 2018 speech, Facebook's Public Policy Director for Global Elections referred to the Philippines as "patient zero" for the fake news phenomenon that targeted the country's presidential elections in 2016.¹²⁴ The use of fake accounts, content farms and 'click armies' for political purposes has since become ubiquitous in political conversations, with disinformation becoming "normalized and professionalized" on all sides of politics.¹²⁵ This domestic disinformation strategy has been described by the Filipino news outlet Rappler (whose editor is being tried for online libel against the government) as 'death by a thousand cuts'. The sheer volume of material questioning facts and

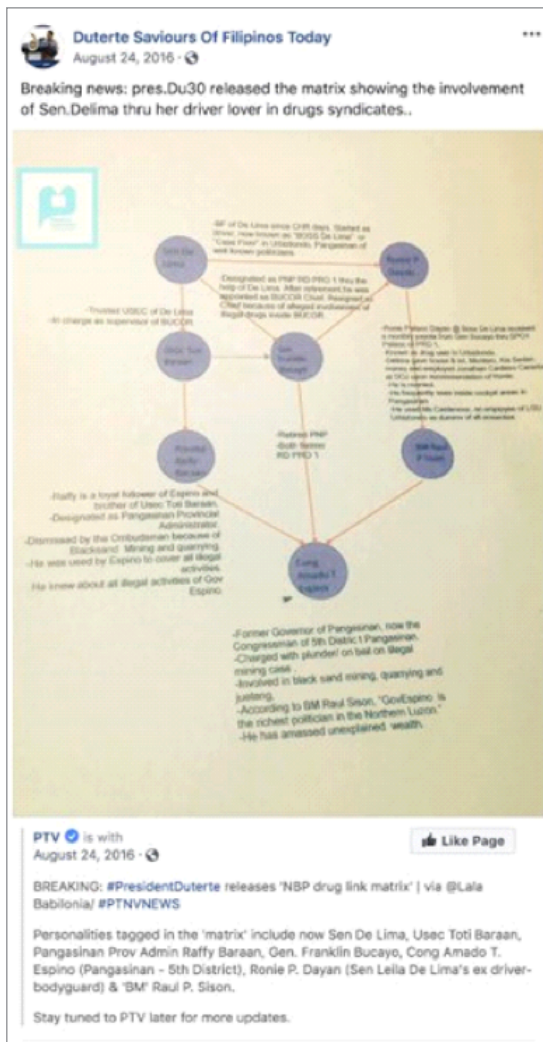
the use of half-truths has been boosted by leveraging bot networks, fake accounts, and platform algorithms on social media to project the desired narrative.¹²⁶

The use of social media to spread hostile narratives raised significant concerns in the lead-up to the May 2019 midterm elections, where a candidate's online presence was a critical factor for electoral success. This came in the wake of reports that President Rodrigo Duterte's office had a budget of USD 200,000 with a staff of 400-500 dedicated to creating promotional material and defending against online criticisms during the 2016 elections and during his presidency.



Disinformation about Duterte's political opponents and accusations of corruption spread from fake Facebook accounts.¹²⁷





Duterte fan accounts being used to amplify claims of conspiracies against political rivals.



A popular Instagram account shared multiple images of a senatorial candidate without context or any disclosure of being a paid post.¹³³

In the aftermath of the 2016 elections, in which allies of President Duterte largely prevailed¹²⁸, researchers found the use of online disinformation was shifting away from clickbait and disinformation, in favor of leveraging relationships with micro-influencers¹²⁹ and online communities¹³⁰, as influencers for hire. The increasingly lucrative 'political trolling industry' in the Philippines

also experienced significant growth.¹³¹ In response to these concerns, the Commission on Elections called for the deliberate spread of misinformation to be considered a form of election fraud and said that it would be watching candidates' spending on 'social media specialists' for campaign spending limit violations.¹³²



Main narratives

Three main narratives emerge from disinformation in the Philippines:

- (a) Narratives about the importance of the so-called ‘War on Drugs’;
- (b) Narratives of corruption to delegitimize political figures;
- (c) Narratives to spread distrust in the mainstream media.

The penetration and saturation of social media have been central to the success of hostile narratives in the Philippines. Many citizens are only able to access the internet through subsidy programs like Facebook Free Basics.¹³⁴ Through partnering with local telecommunications providers, these programs, allow access to a basic suite of online platforms¹³⁵ at no cost to the user. While this can help facilitate greater connectivity and encourage economic growth, these also provide limited content to users, with algorithms often amplifying polarising content while creating radicalizing echo chambers of disinformation.


In response to these concerns, Facebook announced that it was preparing for the elections by working with third-party fact-checkers and machine learning tools to detect disinformation on their platforms. Despite this, the subsequent 2019 midterm election highlighted the shift of online campaigns from the sideline (largely supporting traditional media and physical campaigning) to a key driver of political campaigns. This

marked the first time that digital operations were fully integrated into an overall campaign strategy.¹³⁶

The results of the disinformation phenomenon in the Philippines reach far beyond the content of social media posts. This narrative of ‘fake news’ has been weaponized by both sides of politics, with accusations of disinformation forming a powerful narrative used to undermine political competitors and legitimize excessive use of force. In 2019, arrests for crimes under the 2012 Cyber Crime Prevention Act jumped dramatically, increasing by 292% compared to 2017.¹³⁷ Records of cyber crimes also increased by 80%. Just over 25% of these were online libel cases.¹³⁸



Duterte’s leadership has also seen a number of journalists and individuals charged with online libel in relation to their criticism of the government. This, in combination with regular shutdowns of mobile internet during major events¹³⁹, prompted Freedom House to downgrade the Philippines from “Free” to “Partly Free” in their 2018 “Freedom on the Net” report¹⁴⁰.



<  Lapu-Lapu shared VOVph's post. Yesterday at 10:16 AM · 🌐


HAHAHAHAHAHA GOOD LUCK SPINNING/TWISTING MARIA!

#TryHarder #ImongPanitLuod #VoomSUNOG


 **VOVph** Yesterday at 12:58 AM · 🌐 

Maria Ressa is so desperate to attract attention to her failing blog site from tasteless satire to peddling fake news about dead journalists.

2015 WORLD PRESS FREEDOM INDEX
Rank 141 out of 180


 **Maria Ressa** @mararissa

PH improves in World Press Freedom Index by @maracepeda rappler.com/nation/117586-... via @rapplerdotcom




12:42 AM · 31 Dec 2015

2017 WORLD PRESS FREEDOM INDEX
Rank 127 out of 180

 **Maria Ressa** @mararissa

Philippines 'deadliest country' in Asia for journalists in 2017 – media watchdog | via @rapplerdotcom



Philippines 'deadliest country' in Asia for journalists in ... Reporters Without Borders identified 4 Filipino journalists killed in line with their work in 2017, adding that President Duterte said

6:45 AM · 19 Dec 2017

A Facebook post claiming false reporting from Filipino news outlet Rappler, that has been highly critical of Duterte's presidency.



CONCLUSION

While hostile information activities are far from new tools of statecraft, widespread access to technology and the ease of its use has increased the complexity, scale, and speed in which hostile narratives can spread. However, the success of these operations requires an understanding of an incredibly diverse regional operating environment, including language, cultural nuances, and access to the operating knowledge of a variety of digital platforms alongside a deep familiarity with the stakeholders and adversaries operating in that environment.

This paper has described a range of hostile information activities that attempt to reshape perceptions and influence events both domestically and externally. In countries such as the Philippines and Indonesia, online influence and disinformation is an industry that is used to manipulate domestic public discourse and to legitimize and support government actions such as the ‘war on drugs’. However, hostile information activities are also used to shape how government actions are perceived externally. This can be seen in the various techniques that were used by the professional communications consultancy in Indonesia to shape the international perception of the West Papuan independence movement. Information activities have also been used to interfere in the internal politics of other nations. This is exemplified in the case study of Taiwan,

where the PRC used information activities to attack the opponents of the CCP and justify diplomatic and economic retaliation to silence and repress dissenting views.

Social media companies have in recent years expanded their efforts to prevent their platforms from being abused by hostile information actors, but it is clear that some governments across the region are both victims and perpetrators—sometimes perhaps simultaneously.

Many social media companies appear to focus on tackling hostile information activities in their home markets first, for both political and competency-based reasons. Political pressure to tackle hostile information activities has been greatest in the United States, and these US-based companies understand the culture of their home markets best. Facebook, for example, may be in the best position to detect, understand, and respond to hostile information activities that occur in English-language contexts. Countries in Eastern Asia and other regions of the world, by contrast, have different cultural and linguistic backgrounds that make it more difficult for social media companies to understand and respond appropriately.

The persistent manipulation of information online will not be solved with a single policy initiative or by social media companies



alone. Rather, a robust suite of multifaceted responses is required, including fact-checking, digital literacy and critical thinking-based education, and measures to encourage a strong and independent media with the highest standards of journalistic integrity; measures to encourage civil-society groups to research and transparently uncover hostile information activities; and steps to encourage social media companies to expand their capabilities to detect and remove hostile information activities.



ENDNOTES

- 1 This paper defines eastern Asia as East Asia and Southeast Asia and includes China, Hong Kong, Taiwan, Singapore, South Korea, Japan, Malaysia, Thailand, the Philippines, Vietnam, and Indonesia.
- 2 See Louise Williams and Roland Rich (eds), *Losing Control: Freedom of the Press in Asia* (Canberra: Australian National University E Press, 2013).
- 3 [2019 World Press Freedom Index | Reporters Without Borders.](#) RSF
- 4 Stoycheff, Elizabeth, Erik C. Nisbet, and Dmitry Epstein. 2016. "Differential Effects of Capital-Enhancing and Recreational Internet Use on Citizens' Demand for Democracy." *Communication Research*.
- 5 Funke, Daniel, and Daniela Flamini. "A Guide to Anti-Misinformation Actions around the World." Poynter.
- 6 Wardle, Claire, and Hossein Derakhshan. 2017. "[INFORMATION DISORDER: Toward an Interdisciplinary Framework for Research and Policy Making.](#)" Council of Europe report DGI(2017)09.
- 7 Government of Canada, "[Defence and Security Challenges for second Competitive Projects Call for Proposals: Theme four: Building Cyber Capability](#)".
- 8 Pamment, James, Howard Nothhaft, Henrik Agardh-Twetman, and Alicia Fjällhed. 2018. *Countering Information Influence Activities: The State of the Art* : Research Report. p. 28.
- 9 Hanson, Fergus, Sarah O'Connor, Mali Walker, and Luke Courtois. 2019. [Hacking Democracies](#). Australian Strategic Policy Institute.
- 10 Gleicher, Nathaniel. 2019. "[Removing Coordinated Inauthentic Behavior From China | Facebook Newsroom.](#)". Facebook. Twitter Safety. 2019. "[Information Operations Directed at Hong Kong.](#)" Twitter.
- 11 Roth, Yoel. 2019. "[Information Operations on Twitter: Principles, Process, and Disclosure.](#)"
- 12 Gleicher, Nathaniel. 2019. "[Removing Coordinated Inauthentic Behavior in UAE, Nigeria, Indonesia and Egypt | Facebook Newsroom.](#)". Strick, Benjamin, and Elise Thomas. 2019. [Investigating Information Operations in West Papua](#). Bellingcat.
- 13 Gleicher, Nathaniel. 2018. "[Taking Down Coordinated Inauthentic Behavior in Bangladesh | Facebook Newsroom.](#)" Facebook.
- 14 "[Joint Publication 3-13 Information Operations.](#)" 2012. JCS.
- 15 Stowell, Joshua. 2017. "[India-China Dispute on the Doklam Plateau.](#)" *Global Security Review*.
- 16 Bagchi, Indrani. 2017. "[Doklam Standoff: China Playing out Its 'Three Warfares' Strategy against India.](#)" *The Times of India*.
- 17 Dickie, Mure. 2012. "[Japanese Anti-Nuclear Demonstrations Grow.](#)" *Washington Post*.
- 18 Chao, Vincent. 2014. "[How Technology Revolutionized Taiwan's Sunflower Movement.](#)" *The Diplomat*.
- 19 Parker, Emily. 2014. "[Social Media and the Hong Kong Protests.](#)" *The New Yorker*.
- 20 Friedman, Thomas L. 2019. "[Opinion | Hong Kong's Protests Could Be Another Social Media Revolution That Ends in Failure.](#)" *The New York Times*.
- 21 Ullah Khan, Asif. 2019. "[Brunei: When Sharia Meets Social Media.](#)" *The Diplomat*.
- 22 Abdullah, Najwa, and Amalina Anauer. 2018. "[Old Politics and New Media: Social Media and Malaysia's 2018 Elections.](#)". Shukry, Anisah, and Anuradha Raghu. 2018. "[Mahathir Wins in Historic Malaysia Power Shift.](#)" *Bloomberg.com*.
- 23 Baker, Nick. 2016. "[How Social Media Became Myanmar's Hate Speech Megaphone.](#)" *Myanmar Times*.
- 24 Nguyen, Tram-Anh. 2016. "[Norm or Necessity? The Non-Interference Principle in ASEAN.](#)" *Cornell International Affairs Review* 9(1). ASEAN is the regional intergovernmental Association of Southeast Asian Nations and includes Brunei, Cambodia, Indonesia, Laos, Malaysia, the Philippines, Singapore, Thailand and Vietnam.
- 25 Abbott, Jason P. 2012. "Cacophony or Empowerment? Analysing the Impact of New Information Communication Technologies and New Social Media in Southeast Asia." *Journal of Current Southeast Asian Affairs* 30(4): 3–31. p6.
- 26 Abbott, Jason P. 2012. "Cacophony or Empowerment? Analysing the Impact of New Information Communication Technologies and New Social Media in Southeast Asia." *Journal of Current Southeast Asian Affairs* 30(4): 3–31. p6.
- 27 Sarah Lai Stirland, "['Open-Source Politics' Taps Facebook for Myanmar Protests.](#)" *WIRED*, April 10, 2007,
- 28 New media refers to content made available varying forms of electronic communication made possible through the use of computer technology.
- 29 "[U.S. Army Garrison Humphreys \(Camp Humphreys\).](#)", Facebook., "[U.S. Forces Korea.](#)", Facebook.
- 30 "[U.S. Army Garrison Humphreys \(Camp Humphreys\).](#)", Facebook. , "[U.S. Forces Korea.](#)", Facebook.
- 31 See Louise Williams and Roland Rich (eds), *Losing Control: Freedom of the Press in Asia* (Canberra: Australian National University E Press, 2013).
- 32 "[2019 World Press Freedom Index | Reporters Without Borders.](#)" RSF.
- 33 Pirannejad, Ali. 2017. "Can the Internet Promote Democracy? A Cross-Country Study Based on Dynamic Panel Data Models." *Information Technology for Development* 23(2): 281–95. and Nisbet, Erik C., Elizabeth Stoycheff, and Katy E. Pearce. 2012. "Internet Use and Democratic Demands: A Multinational, Multilevel Model of Internet Use and Citizen Attitudes About Democracy." *Journal of Communication* 62(2): 249–65.



- 34 Shahbaz, Adrian. 2018. ["Freedom on the Net 2018: The Rise of Digital Authoritarianism."](#)
- 35 Stoycheff, Elizabeth, Erik C. Nisbet, and Dmitry Epstein. 2016. "Differential Effects of Capital-Enhancing and Recreational Internet Use on Citizens' Demand for Democracy." *Communication Research*: 0093650216644645.
- 36 ["Understanding Social Media and Conflict | Facebook Newsroom."](#)
- 37 Wanless, Alicia, and Michael Berk. 2017. ["Participatory Propaganda: The Engagement of Audiences in the Spread of Persuasive Communications."](#)
- 38 Funke, Daniel, and Daniela Flamini. ["A Guide to Anti-Misinformation Actions around the World."](#) Poynter.
- 39 According to the 2019 Global Digital Report by We Are Social and Hootsuite
- 40 ["Digital 2019: Global Digital Overview."](#) DataReportal – Global Digital Insights.
- 41 ["Digital 2019: The Philippines."](#) DataReportal – Global Digital Insights.
- 42 ["Digital 2019: Japan."](#) DataReportal Global Digital Insights.
- 43 ["Digital 2019: Global Digital Overview."](#) DataReportal – Global Digital Insights.
- 44 ["Free Basics."](#) 2018. Facebook Connectivity.
- 45 ["Loon."](#) Loon.
- 46 ["Digital 2019 in China."](#) We Are Social China.
- 47 ["Digital 2019: Indonesia."](#) DataReportal – Global Digital Insights.
- 48 ["Digital 2019: The Philippines."](#) DataReportal – Global Digital Insights.
- 49 ["Digital 2019: Taiwan."](#) DataReportal – Global Digital Insights.
- 50 PTT is not present in these statistics as it is classified as a bulletin board system, not a social media.
- 51 Albert, Eleanor. 2019. ["China-Taiwan Relations."](#) Council on Foreign Relations.
- 52 Kania, Elsa. 2016. ["The PLA's Latest Strategic Thinking on the Three Warfares."](#) Jamestown.
- Mattis, Peter. 2018. ["China's 'Three Warfares' in Perspective."](#) War on the Rocks.
- 53 Hayton, Bill. 2014. ["China's False Memory Syndrome."](#)
- Truite, Kevin. 2019. ["China's Narrative Warfare in East Asia."](#) Georgetown Security Studies Review and
- 54 Hille, Kathrin. 2019. ["Beijing's Simplistic Narrative on Taiwan Is Fuelling Tensions."](#) Financial Times.
- 55 King, Gary, Jennifer Pan, and Margaret E. Roberts. 2017. "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument." *American Political Science Review* 111(3): 484–501.
- 56 Mechkova, Valeriya, Daniel Pemstein, Brigitte Seim, and Steven Wilson. 2019. ["Measuring Internet Politics: Introducing the Digital Society Project."](#) Digital Society Project.
- 57 Chien, Huang, and Hsieh Chun-lin. 2018. ["Prosecutors: China Paid Wang for Propaganda."](#) Taipei Times.
- 58 Cave, Danielle. 2018. ["Cyber-Enabled Information and Influence Operations—It's Not Just Russia."](#) The Strategist
- 59 Chen, Ketty W., and J. Michael Cole. 2019. ["CCP and Proxy Disinformation: Means, Practices, and Impact on Democracies."](#) Synopsis.
- 60 Chen, Ketty W., and J. Michael Cole. 2019. ["CCP and Proxy Disinformation: Means, Practices, and Impact on Democracies."](#) Synopsis.
- 61 Chen, Ketty W., and J. Michael Cole. 2019. ["CCP and Proxy Disinformation: Means, Practices, and Impact on Democracies."](#) Synopsis.
- 62 Chen, Ketty W., and J. Michael Cole. 2019. ["CCP and Proxy Disinformation: Means, Practices, and Impact on Democracies."](#) Synopsis.
- 63 Paul, Huang, 2019 ["Chinese Cyber-Operatives Boosted Taiwan's Insurgent Candidate"](#), Foreign Policy.
- 64 Paul, Huang, 2019 ["Chinese Cyber-Operatives Boosted Taiwan's Insurgent Candidate"](#), Foreign Policy.
- 65 I-fan, Lin. 2018. ["Made-in-China Fake News Overwhelms Taiwan."](#) Global Voices Advocacy.
- 66 I-fan, Lin. 2018. ["Made-in-China Fake News Overwhelms Taiwan."](#) Global Voices Advocacy
- 67 I-fan, Lin. 2018. ["Made-in-China Fake News Overwhelms Taiwan."](#) Global Voices Advocacy
- 68 Chen, Ketty W., and J. Michael Cole. 2019. ["CCP and Proxy Disinformation: Means, Practices, and Impact on Democracies."](#) Synopsis.
- 69 Everington, Keoni. 2019. ["Taiwan Is Main Target of China's Disinformation"](#) Taiwan News.
- 70 I-fan, Lin. 2018. ["Made-in-China Fake News Overwhelms Taiwan."](#) Global Voices Advocacy
- 71 Ping-Hung, Chen. 2018. ["We Should Teach Media Literacy to All Students - Taipei Times."](#) Taipei Times.
- 72 White, Edward. 2019. ["Taiwan Warns of 'Rampant' Fake News amid China Interference Fears."](#) Financial Times.
- 73 Feldman, Brian. 2018. "Wikipedia Is Not Going to Save YouTube From Misinformation." *Intelligencer*. <http://nymag.com/intelligencer/2018/03/youtube-will-use-wikipedia-for-fact-checking.html>; Flynn, Kerry. 2017.
- 74 Miller, Carl. 2019. ["China and Taiwan Clash over Wikipedia Edits - BBC News."](#) BBC News.
- 75 Miller, Carl. 2019. ["China and Taiwan Clash over Wikipedia Edits - BBC News."](#) BBC News.
- 76 Twitter Safety. 2019. ["Information Operations Directed at Hong Kong."](#) Twitter.
- 77 Gleicher, Nathaniel. 2019. ["Removing Coordinated Inauthentic Behavior From China | Facebook Newsroom."](#)
- 78 Roth, Yoel. 2019. ["Information Operations on Twitter: Principles, Process, and Disclosure."](#) Twitter.
- 79 See <https://webkay.robinlinus.com/> and <https://panopticklick.org/> for a demonstration of what information a web site can learn from a browser.



- 80 Uren, Tom, Elise Thomas, and Jacob Wallis. 2019. ["Tweeting through the Great Firewall."](#) Aspi.org.au.
- 81 Uren, Tom, Elise Thomas, and Jacob Wallis. 2019. ["Tweeting through the Great Firewall."](#) Aspi.org.au.
- 82 ["Freedom on the Net 2018: The Rise of Digital Authoritarianism."](#) Freedomhouse.
- 83 Li, Audrey Jiajia. 2019. ["Opinion | Who's Afraid of China's Internet Vigilantes?"](#) The New York Times.
- 84 King, Gary, Jennifer Pan, and Margaret E. Roberts. 2017. "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument." *American Political Science Review* 111(3): 484–501.
- 85 Uren, Tom, Elise Thomas, and Jacob Wallis. 2019. ["Tweeting through the Great Firewall."](#) Aspi.org.au.
- 86 "It's Madness': Hong Kong Police Say They're 'trapped in the Middle' amid Unprecedented Unrest." 2019. ABC News. <https://www.abc.net.au/news/2019-06-15/hong-kong-police-say-they-are-trapped-in-the-middle/11212832>
- 87 Uren, Tom, Elise Thomas, and Jacob Wallis. 2019. ["Tweeting through the Great Firewall."](#) Aspi.org.au.
- 88 Uren, Tom, Elise Thomas, and Jacob Wallis. 2019. ["Tweeting through the Great Firewall."](#) Aspi.org.au.
- 89 Uren, Tom, Elise Thomas, and Jacob Wallis. 2019. ["Tweeting through the Great Firewall."](#) Aspi.org.au.
- 90 Uren, Tom, Elise Thomas, and Jacob Wallis. 2019. ["Tweeting through the Great Firewall."](#) Aspi.org.au.
- 91 Uren, Tom, Elise Thomas, and Jacob Wallis. 2019. ["Tweeting through the Great Firewall."](#) Aspi.org.au.
- 92 Forsythe, Michael. 2017. ["Billionaire Who Accused Top Chinese Officials of Corruption Asks U.S. for Asylum."](#) The New York Times.
- 93 Hilgers, Lauren. 2018. ["The Mystery of the Exiled Billionaire Whistle-Blower."](#) The New York Times.
- 94 Edens, Rob. 2019. ["How Beijing and Others Weaponized Interpol and the Magnitsky Act."](#)
- 95 Barboza, David. 2018. ["Steve Bannon and a Fugitive Billionaire Target a Common Enemy: China."](#) The New York Times.
- 96 O'Keefe, Aruna Viswanatha and Kate. 2019. ["Chinese Tycoon Holed Up in Manhattan Hotel Is Accused of Spying for Beijing."](#) Wall Street Journal.
- 97 Uren, Tom, Elise Thomas, and Jacob Wallis. 2019. ["Tweeting through the Great Firewall."](#) Aspi.org.au.
- 98 Uren, Tom, Elise Thomas, and Jacob Wallis. 2019. ["Tweeting through the Great Firewall."](#) Aspi.org.au.
- 99 Phillips, Tom. 2017. ["Bookseller Gui Minhai 'half Free' after Being Detained in China for Two Years."](#) The Guardian.
- 100 Sui, Phila. 2018. ["Sweden 'Using Me like Chess Piece'. Says Detained Publisher Gui Minhai in Government-Arranged Interview."](#) South China Morning Post.
- 101 Phillips, Tom. 2018. ["Bookseller Gui Minhai Surfaces in Chinese Custody to Deliver Staged Confession."](#) The Guardian.
- 102 Uren, Tom, Elise Thomas, and Jacob Wallis. 2019. ["Tweeting through the Great Firewall."](#) Aspi.org.au.
- 103 Uren, Tom, Elise Thomas, and Jacob Wallis. 2019. ["Tweeting through the Great Firewall."](#) Aspi.org.au.
- 104 Badenhansen, Kurt, and Mike Ozanian. 2019. ["NBA Team Values 2019: Knicks On Top At \\$4 Billion."](#) Forbes.
- 105 Zillgitt, Jeff, and Mark Medina. ["As Impasse over Pro-Hong Kong Tweet Simmers, What's at Stake for the NBA in China?"](#) USA TODAY.
- 106 Novy-Williams, Eben. 2019. ["NBA China Woes Threaten Billions of Dollars. Decades' Work."](#) Bloomberg.com.
- 107 McNicol, Andrew. 2017. ["How the NBA Became the Most Popular Sports League in China."](#) South China Morning Post.
- 108 Thompson, Ben. 2019. ["The China Cultural Clash."](#) *Stratechery* by Ben Thompson.
- 109 Cohen, Ben, Georgia Wells, and Tom McGinty. 2019. ["How One Tweet Turned Pro-China Trolls Against the NBA."](#) Wall Street Journal.
- 110 Cohen, Ben, Georgia Wells, and Tom McGinty. 2019. ["How One Tweet Turned Pro-China Trolls Against the NBA."](#) Wall Street Journal.
- 111 Wang, Yaqiu. 2018. ["China's Social Media Crackdown Targets Twitter."](#) Human Rights Watch.
- 112 Kharpal, Arjun. 2019. ["Chinese State Media and Tencent Suspend Broadcast of NBA Preseason Games in China."](#) CNBC.
- 113 Toh, Michelle, and Laura He. 2019. ["All of the NBA's Official Chinese Partners Have Suspended Ties with the League."](#) CNN.
- 114 Yue, Zhang. 2019. ["China's Basketball Association Suspends Cooperation with Rockets - Chinadaily.Com.Cn."](#) China Daily. (October 26, 2019).
- 115 ["Transcript of Foreign Ministry Spokesperson Geng Shuang's Regular Press Conference on the Erroneous Comments on Hong Kong by General Manager of the Houston Rockets."](#) 2019. Houston. China Consulate
- 116 ["Global Brands Better Stay Away from Politics - Global Times."](#) 2019. Global Times.
- 117 Potkin, Fanny, and Agustinus Beo Da Costa. 2019. ["In Indonesia, Facebook and Twitter Are 'buzzed' Battlegrounds as Elections Loom."](#) Reuters.
- 118 Soeriaatmadja, Wahyudi. 2017. ["Indonesian Police Probe Alleged Fake News Factory's Protest Links."](#) The Straits Times
- 119 Strick, Benjamin. 2019. ["Investigating Information Operations in West Papua: A Digital Forensic Case Study of Cross-Platform Network Analysis."](#) Bellingcat.
- 120 Tapsell, Ross. 2019. "Singapore | 20 September 2019 Indonesia's Policing of Hoax News Increasingly Politicised." *Perspective* 75(2019): p10.
- 121 Costa, Agustinus Beo Da. 2019. ["Indonesia Lifts Social Media Curbs Targeting Hoaxes during Unrest."](#) The Star Online.
- 122 Strick, Benjamin. 2019. ["Investigating Information Operations in West Papua: A Digital Forensic Case Study of Cross-Platform Network Analysis."](#) Bellingcat.



- 123 [“Removing Coordinated Inauthentic Behavior in UAE, Nigeria, Indonesia and Egypt | Facebook Newsroom.”](#) 2019.
- 124 Rappler, [‘360/OS: Facebook’s Katie Harbath on protecting election integrity’](#), Youtube, June 23rd 2018,
- 125 Ong, Jonathan Corpus and Jason Vincent A Cabanes. ‘Architects of Networked Disinformation: Behind the Scenes of Troll Accounts and Fake News Production in the Philippines’. University of Leeds, Newton Tech4Dev Network, February 9th 2018.
- 126 Ressa, Maria A. [“Propaganda War: Weaponizing the Internet.”](#) Rappler.
- 127 Smith, Melanie. 2019. [“Archives: Facebook Finds ‘Coordinated and Inauthentic Behavior’ In the Philippines: Suspends a Set of Pro-Government Pages Ahead of May Elections.”](#) Medium.
- 128 [“Philippines: President Duterte’s Allies Dominate Senate Race.”](#) 2019. Al Jazeera.
- 129 Ong, Jonathan Corpus, Ross Tapsell, and Nicole Curato. 2019. [Tracking Digital Disinformation in the 2019 Philippine Midterm Election](#). New Mandala.
- 130 Ong, Jonathan Corpus, Ross Tapsell, and Nicole Curato. 2019. [Tracking Digital Disinformation in the 2019 Philippine Midterm Election](#). New Mandala.
- 131 Ong, Jonathan Corpus, Ross Tapsell, and Nicole Curato. 2019. [Tracking Digital Disinformation in the 2019 Philippine Midterm Election](#). New Mandala.
- 132 Tomacruz, Sofia. 2018. [“‘Fake News’ Should Be Considered Form of Election Fraud, Says Watchdog.”](#) Rappler.
- 133 Silverman, Craig. 2019. [“‘Patient Zero’: The Philippines Offers A Preview Of The Disinformation Tactics The US Could See In 2020.”](#) BuzzFeed News.
- 134 [“Free Basics.”](#) 2018. Facebook Connectivity.
- 135 Mateo, Janvic. [‘Facebook to protect integrity of 2019 midterm elections’](#). The Philippine Star, January 26th 2019
- 136 Ong, Jonathan Corpus, Ross Tapsell and Nicole Curato. [‘Tracking Digital Disinformation in the 2019 Philippine Midterm Election’](#), New Mandala, August 2019, pp.21
- 137 Tupas, Emmanuel. [‘Cybercrime arrests up by 291% in 2018’](#), The Philippine Star Global, April 8th 2019.
- 138 Tupas, Emmanuel. [‘Cybercrime arrests up by 291% in 2018’](#), The Philippine Star Global, April 8th 2019.
- 139 Ballaran, Jhoanna. [‘Group criticizes gov’t move shutting down cellphone signals during events.’](#) Inquirer.net, January 26th 2018,; Letigio, Delta Dyrecka. [‘NTC says only ‘shutoff’ not ‘shutdown’ of mobile, internet signals during Sinulog 2019 events’](#). Cebu Daily News, January 7th 2019.
- 140 Freedom House. ‘Freedom on the Net 2018 – Philippines’, Freedom on the Net.



