Understanding global disinformation and information operations

Insights from ASPI's new analytic website

Ingram Niblock, Dr Jacob Wallis, and Albert Zhang

Executive summary

ASPI's International Cyber Policy Centre has launched the *Understanding Global Disinformation and Information Operations* website alongside this companion paper. The site provides a visual breakdown of the publically-available data from state-linked information operations on social media. ASPI's Information Operations and Disinformation team has analysed each of the data sets in Twitter's Information Operations archive to provide a longitudinal analysis of how each state's willingness, capability and intent has evolved over time. Our analysis demonstrates that there is a proliferation of state actors willing to deploy information operations targeting their own domestic populations, as well as those of their adversaries. We find that Russia, Iran, Saudi Arabia, China and Venezuela are the most prolific perpetrators. By making these complex data sets available in accessible form ASPI is broadening meaningful engagement on the challenge of state actor information operations and disinformation campaigns for policymakers, civil society and the international research community.

Since October 2018, Twitter has released the tweets, media and details of associated accounts that the social network believes were part of state-linked information operations. The datasets originated from 17 countries, including the usual suspects Russia, China and Iran, but also Armenia, Bangladesh, Cuba, Ecuador, Egypt, Honduras, Indonesia, Serbia, Spain, Thailand, Turkey, the United Arab Emirates and Venezuela.

Analysis of information operations that exploit social media as a vector has tended towards the examination of individual sets of takedown data, particularly those relating to high-profile significant state actors (such as Russia, China and Iran). Few research entities have the technical and analytical capability to investigate more complex takedown datasets, hindering our capacity to understand the tactics and tradecraft of actors willing to mobilise strategic deception as a tool of statecraft. Yet traits within this data help us determine who was responsible, who the targets were, the narratives propagated and the patterns of coordination and inauthentic behaviour.

Twitter's Information Operations Archive now has sufficient longitudinal data for us to learn more about how actors behave over time. To that end, ASPI has built this unique website to analyse and compare all the data from the Information Operations Archive at the same time. Policymakers and researchers can now consistently compare the activity, techniques and narratives across each operation, and compare what states do differently from each other and how their activities change over time.

Twitter has been perhaps the most forward-leaning entity in the social media industry in terms of its public engagement on information operations. No other company has consistently provided complete state-actor-linked information operations datasets for public scrutiny. Twitter's recent signalling that it will discontinue the Information Operations Archive makes ASPI's longitudinal analysis of these datasets all the more pertinent.

March 2022

Analysing information operations on Twitter

Actors engaged in information operations in Twitter's archive have usually been found to be engaging in platform manipulation. Platform manipulation policies focus on the behaviour of the accounts rather than the content posted, as it's difficult to decisively act on content alone. A controversial opinion may be both genuinely held by a group in a society who legitimately contribute to the debate and exploited by foreign states manipulating the platform and seeking to inflame divisions. Interference in the 2016 and 2020 US elections is an example here.

On Twitter, platform manipulation takes a number of forms that exploit the way content is discovered and goes viral. Some basic techniques include repeatedly using a hashtag so that Twitter users see that it is trending and are curious enough to find out more. Another basic technique to boost content is to repeatedly retweet a particular message so that it looks more popular than it really is. Fundamentally, Twitter's policy is designed to protect against coordinated deception at scale.

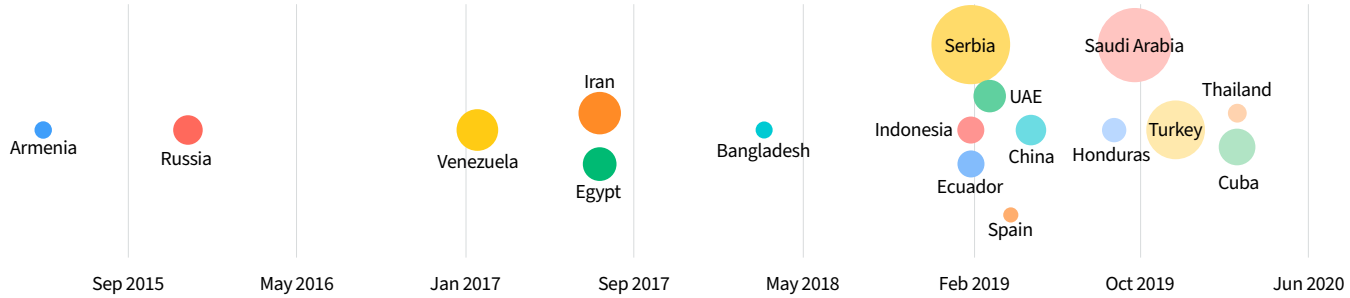
ASPI's analysis has extracted key indicators of activity on Twitter in order to characterise how countries conduct their information operations, and we've also run machine-learning algorithms over the datasets to extract entities and identify language sets used in the tweet data. Mentions of places and countries provide an indication of targeted countries in those information operations and act as a rough cut of the data to guide future focused research.

Analysing Twitter Information Operations Archive data can be complex. Datasets may be large, and there's typically gigabytes, and sometimes terabytes, of media. ASPI used cloud technologies to store, manipulate and visualise all the datasets in the archive and process the raw data in detail, allowing analysts to generate new hypotheses and insights.

One novel approach ASPI took was to restrict the datasets to tweets posted by the suspended accounts within the last 90 days of an account's last tweet. ASPI's analysis found that this filter included only the most relevant content, as many of the accounts in the datasets were probably repurposed or purchased, and their earlier tweets contained commercial content that was not of interest in the scope of this work.The earlier data often skewed the apparent behaviour of the accounts and could also make it difficult to identify and assess the most significant content shared in the datasets.

What did ASPI find in the data?

Peak activity



Timeline of when the most tweets were sent by operations originating from each country. The size of the circle is the relative to the number of tweets sent. Source: ASPI analysis

Although it's a relatively simple metric, the months when the number of tweets peaked for each country provides a useful timeline showing how these operations slowly became more popular and, in some cases, increased in scale.

Of the top five campaigns (selected by number of takedowns), it's no surprise that campaigns originating in Russia were the first to peak in December 2015, with 140,298 tweets sent that month, mostly in Russian and English. Events around that time included an uptick of Russian involvement in the Syrian civil war, the announcement of Russia's ban from the 2016 Olympics for doping and the upcoming US presidential election in 2016.

In 2017, activity originating from Venezuela and Iran peaked in February and August, respectively. At their most active, those two operations were churning out 485,821 and 519,369 tweets—a significant uptick compared to Russia's peak two years earlier.

In a sign that information operations on social media had gone mainstream, nine operations reached their apex in 2019. Of the top five countries in this report, operations originating from China and Saudi Arabia had their peak in May and October, respectively. Saudi Arabian actors sent 2.3 million tweets that month, while operatives in China sent a comparatively restrained 158,611.

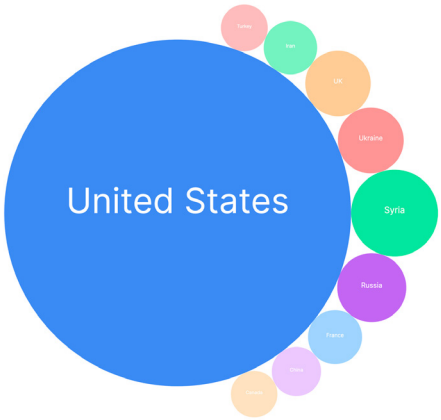
However, an operation that originated in Serbia sent the most tweets in one month: 2.7 million tweets in February 2019.

The top five

Russia

By the numbers	
Number of takedowns	8 (1st)
Number of accounts in all datasets	5,361 (6th)
Total number of tweets (90-day filter)	754,367 (6th)
Peak of activity	December 2015 (140,298 tweets)

Source: ASPI



Relative mentions of countries in tweets that originated from Russia.

Between October 2018 and March 2021, Twitter removed eight networks that it believes originated in Russia and were attributed to the Internet Research Agency and other Russian state actors. ASPI's analysis of all Russia-linked operations found that mentions of the US dwarfed those of all other countries and that the most used hashtags were heavily focused n hot-button US political issues, including President Trump's 'MAGA' slogan, QAnon and anti-Islam sentiment.

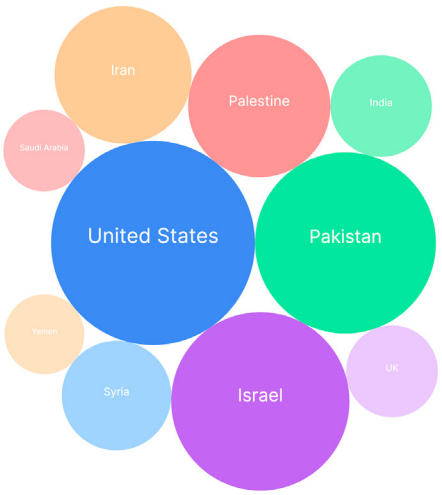
US domestic politics wasn't the only focus. Other narratives included efforts to undermine NATO to European audiences, slander Ukrainian leaders, promote Russian foreign and military policy in Syria, and discredit candidates in US and European democratic elections.

Russian operations amplified content from Russian state-linked media and operated across social media platforms. Russian assets impersonated media outlets, politicians, activists, government agencies and other organisations.

Iran

By the numbers	
Number of takedowns	7 (2nd)
Number of accounts in all datasets	8,211 (4th)
Total number of tweets (90-day filter)	2,724,125 (4th)
Peak of activity	August 2017 (519,369 tweets)

Source: ASPI



Relative mentions of countries in tweets that originated from Iran

Between November 2019 and March 2021, Twitter removed seven networks it believed originated in Iran and were backed by or associated with the Iranian Government. Given that Twitter is banned in Iran, the campaigns sought to influence international perceptions of Iran while stirring up political division and encouraging unrest in adversary states. These networks also amplified content relating to social divisions in the US, such as the Black Lives Matter movement.

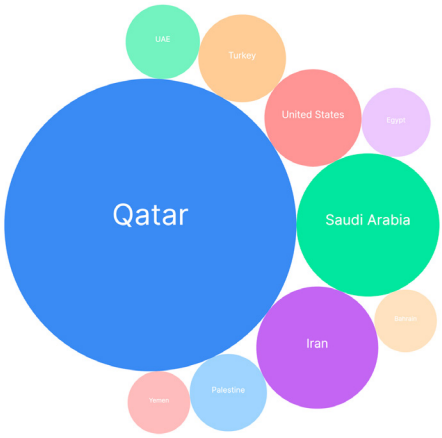
Unlike Russia-linked messaging—which was overwhelmingly focused on the US—Iran-linked messaging referenced countries in Iran's region, including Pakistan, Palestine, Israel and Syria.

The network's fake personas were sometimes convincing, well-rounded characters, giving the appearance of locals concerned with particular political issues. Other assets may have been part of an 'influence for hire' network. Some of those networks benefited from Iran's sophisticated fake news and state media apparatus.

Saudi Arabia

By the numbers	
Number of takedowns	4 (3rd)
Number of accounts in all datasets	11,318 (2nd)
Total number of tweets (90-day filter)	41,201,791 (1st)
Peak of activity	October 2019 (2,316,045 tweets)

Source: ASPI



Relative mentions of countries in tweets that originated from Saudi Arabia

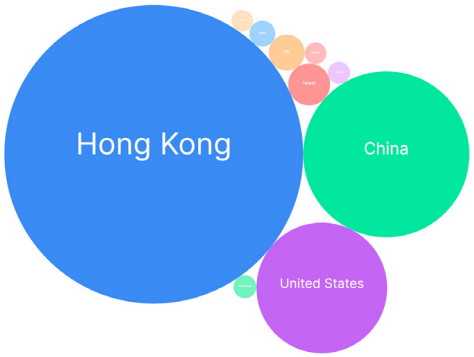
Between October 2019 and January 2020, Twitter removed four networks of accounts associated with Saudi Arabia and in some cases linked to Saudi Arabian state-run media. In general, accounts in the networks primarily sought to advance the foreign policy aims of the Saudi Government, praise the Saudi leadership and shape perceptions about domestic and international issues occurring in the Gulf countries, such as the Yemen civil war.

As evidenced by the number of mentions of Qatar relative to other states, Saudi-linked accounts were most prolific in the politically tense period of the Qatar blockade, when Qatar was isolated by Saudi Arabia, Egypt, Bahrain and the United Arab Emirates, starting in 2017.

China

By the numbers	
Number of takedowns	3 (equal 4th)
Number of accounts in all datasets	28,991 (1st)
Total number of tweets (90-day filter)	2,193,582 (6th)
Peak of activity	May 2019 (158,611 tweets)

Source: ASPI



Relative mentions of countries in tweets that originated from China

Between September 2019 and July 2020, Twitter removed three networks of accounts that originated within China, which is notable, given that the platform is blocked to the majority of the population in the country. In terms of geographical mentions, Hong Kong dominated the data compared with mentions of China itself and the US.

The networks disclosed in these datasets generally sought to influence the attitudes of Chinese diaspora communities and citizens overseas on domestic and foreign policy issues that were of concern to the Chinese Communist Party. Tweets contained both simplified Chinese text, which is used by Chinese citizens originating from the Chinese mainland, and traditional Chinese text, which is used in Hong Kong and Taiwan. Notably, the posting pattern for the China-origin tweets almost perfectly mapped to Chinese working hours, with a peak of posting at 10 am and a lunch break around noon.

Venezuela

Number of takedowns	3 (equal 4th)
Number of accounts in all datasets	1,993 (10th)
Total number of tweets (90-day filter)	2,403,772 (5th)
Peak of activity	February 2017 (485,821 tweets)

Between March and July 2019, Twitter removed three networks of accounts that originated from Venezuela. The tweets amplified content supportive of the government of President Nicolás Maduro for domestic Venezuelan audiences and shared news content that aligned with government foreign policy positions on the US. They also targeted political activists and expressed support for the Venezuelan military.

The future of information operations research

Finding, understanding and combating information operations is a collective effort involving civil society, academia, technology platforms and government. This work is only likely to increase as more state and non-state actors enter this space to achieve their own foreign and domestic goals. Overarching studies of the field of information operations analysis highlight the limited international capacity—beyond a handful of centres of excellence—to analyse information operations data. It's with a view to capacity building that we offer our analysis of the available empirical data on attributed state-actor information operations.

By breaking down the datasets into component parts, we hope to offer the broader international community a gateway into the analysis of these complex datasets. Our effort offers others in the field not just access to data but also some transparency about the approaches to analysis that we find useful.

Each organisation looking at information operations will have its own mandate and focus. Governments are often narrowly confined to the national security space so that they can't be accused of meddling in legitimate domestic political discourse. But domestic disinformation operations will continue to be a huge concern and should be investigated by civil society, academia and the media.

All of this requires continued transparency and access to data from social media platforms — and preferably from multiple platforms. All the more so because the tradecraft will improve as low-quality campaigns are detected early by the social media companies. Collaboration—particularly between civil society and the platforms—is a must to enable attribution and deterrence. High-quality attribution requires access to non-public data that only social media companies hold (such as login information, emails and IP addresses). That data can be a breadcrumb trail to the source of the campaign. But this information is rightly private and shouldn't be carelessly shared—including with governments—without proper authority, oversight and governance. The strongest attribution will be collective, when industry, governments and civil society organisations join to present high-confidence judgements based on shared, understood, empirical data.

We need a combination of cross-sectoral collaboration and societal resilience to defend against information operations. The *Understanding Global Disinformation and Information Operations* website is an example of how the private and not-for-profit sectors can cooperate productively.

About the author

Ingram Niblock is an Analyst with ASPI's International Cyber Policy Centre.
Dr Jacob Wallis is Head of Program, Information and Operations and Disinformation with ASPI's International Cyber Policy Centre.
Albert Zhang is a Researcher with ASPI's International Cyber Policy Centre.

Acknowledgements

Thank you to Michael Shoebridge, Fergus Hanson and our external reviewer for their comments and feedback on the development of this paper. We are grateful to the Institute for War and Peace Reporting for supporting this research project. This project was funded through grants totalling US$129,000 from the US Department of State.

What is ASPI?

The Australian Strategic Policy Institute was formed in 2001 as an independent, non-partisan think tank. Its core aim is to provide the Australian Government with fresh ideas on Australia's defence, security and strategic policy choices. ASPI is responsible for informing the public on a range of strategic issues, generating new thinking for government and harnessing strategic thinking internationally. ASPI's sources of funding are identified in our Annual Report, online at www.aspi.org.au and in the acknowledgements section of individual publications. ASPI remains independent in the content of the research and in all editorial judgements.

ASPI International Cyber Policy Centre

ASPI's International Cyber Policy Centre (ICPC) is a leading voice in global debates on cyber, emerging and critical technologies, issues related to information and foreign interference and focuses on the impact these issues have on broader strategic policy. The centre has a growing mixture of expertise and skills with teams of researchers who concentrate on policy, technical analysis, information operations and disinformation, critical and emerging technologies, cyber capacity building, satellite analysis, surveillance and China-related issues.

The ICPC informs public debate in the Indo-Pacific region and supports public policy development by producing original, empirical, data-driven research. The ICPC enriches regional debates by collaborating with research institutes from around the world and by bringing leading global experts to Australia, including through fellowships. To develop capability in Australia and across the Indo-Pacific region, the ICPC has a capacity building team that conducts workshops, training programs and large-scale exercises for the public and private sectors.

We would like to thank all of those who support and contribute to the ICPC with their time, intellect and passion for the topics we work on. If you would like to support the work of the centre please contact: icpc@aspi.org.au

Important disclaimer

ASPI

Tel +61 2 6270 5100
Email enquiries@aspi.org.au
www.aspi.org.au
www.aspistrategist.org.au
facebook.com/ASPI.org
@ASPI_ICPC

First published March 2022. ISSN 2209-9689.

Funding support for this publication was provided by the US Department of State.


ASPI
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE
INTERNATIONAL
CYBER POLICY
CENTRE