Canadian Security Intelligence Service | Service canadien du renseignement de sécurité

TOP SECRET/

INTELLIGENCE ASSESSMENT

China's Next-Generation Propaganda Machine Poses an Emerging Threat

Intelligence Assessments Branch
Direction de l'évaluation du renseignement

Canada

INTELLIGENCE ASSESSMENT

2021 10 20 TOP SECRET/ CSIS IA 2021-22/59

China's Next-Generation Propaganda Machine Poses an Emerging Threat

This forward-looking IA has been produced by It is meant to inform government decision makers on the future impacts on the PRC's expanding capability to conduct online influence activity. It is a follow-up piece to CSIS IA 2021-22/24 China's Expanding Digital Collection: A Global Strategic Threat

In direct response to the desires of Communist Party of China (CPC) officials, companies from the People's Republic of China (PRC) are developing "smart" propaganda platforms that leverage artificial intelligence (AI) and big data analytics to efficiently exploit Western social media sites, with the aim of shaping the opinions and behaviours of billions of users. that this next-generation approach to propaganda production and dissemination represents an emerging threat that will give the PRC greater ability to undermine facts, democratic principles and public confidence in Western media and institutions. (TS/

Key Assessments

-
-
- *Developers of smart propaganda platforms aim to leverage AI to silence China's most vocal and influential critics.*
-
- The promised capabilities of Chinese-made smart propaganda platforms far exceed conventional online propaganda practices. When fully developed, these platforms potentially represent a new standard in propaganda systems that will permit the PRC to more effectively influence those in other countries. Technical challenges that may hinder the PRC's progress in effectively implementing these tools are expected to be resolved as capabilities increase over the next five years. While the PRC will most likely address these challenges using domestic technologies, it is also possible that PRC actors will illicitly target and acquire foreign technologies, including those originating from Canada and its allies. (S)

What makes online propaganda 'smart'?

1. The production and dissemination of online propaganda is a deliberate and systematic attempt to influence and shape perceptions, manipulate attitudes and beliefs, and direct behaviour to achieve a desired response. This process is made "smart" through the application of artificial intelligence (AI) and big data analysis. By deploying AI algorithms, automation and psychographic profiling,[1] state actors can dramatically improve their abilities to (i) quickly identify undesirable online sentiments before they go viral; (ii) rapidly produce tailored counter-responses; (iii) identify specific audiences that are most receptive to the content; and, (iv) optimize amplification of that content with a view to making it an accepted "truth" among large populations. (U)

Why is this an emerging threat?

2. Applying psychographic profiling to large groups of social media users can reveal deeply personal and granular details about each individual; this information can then be used to micro-target and emotionally influence the way those users think and make decisions. This process was applied by the firm Cambridge Analytica when it micro-targeted tens of millions of unwitting social media users with tailored messaging during the 2016 presidential election in the United States and the 2016 Brexit referendum in the United Kingdom. Some observers maintain that the work of Cambridge Analytica influenced the outcome of both events. (U)

How does this impact Canada?

4. Once these tools are fully developed and their full suite of capabilities realized, they will likely be deployed in influence operations that reach beyond China's immediate geographic sphere, thereby serving to undermine Canadian values and social cohesion, including popular support for Canadian political leaders and major decisions/announcements they make.

Application	Estimated number of Canadian users (2021)
Facebook	25.1 million
YouTube	17.6 million*
Instagram	12.6 million
Twitter	7.6 million
TikTok	3.2 million*
WeChat	1 million

*Avg. number of monthly visitors

(TS/

1 Psychographics describe the cognitive traits of humans such as attitudes, interests, opinions and belief, as well as overt behaviour. Many of these traits can be gathered online to develop a psychographic profile, which may include the analysis of an individual's sentiment expressed in various online forums (e.g., Twitter, Facebook). (U)

Developers of smart propaganda platforms aim to leverage AI to silence China's most vocal and influential critics

-
-
-

Smart propaganda platforms have several foreign interference applications

Foreign elections

-

- Open sources indicate the PLA's Strategic Support Force (SSF) leveraged Western social media as part of an influence operation directed at Taiwan's local elections in November 2018. Observers assess that the PLA sought to control social media narratives in the lead-up to the election. Such efforts are expected to become more sophisticated over time, with more credible content that will be increasingly difficult to trace back to the PRC. (U)
-

Psychological operations

-
- The above capabilities can inform potential operations that target the social media accounts of adversaries with disinformation that aims to undermine morale, sow confusion and degrade decision-making. This approach to cognitive domain operations (CDO) was discussed by researchers from the National University of Defense Technology (NUDT) in a 2018 article. Authors stated the importance of applying CDO to social media and called for more research into how Facebook and Twitter can be exploited in this way. (U)
- An article from October 2018 by PLA SSF members[2] referenced hardware requirements that could support CDO, including "voice information synthesis technology", which can manipulate audio or video clips. Such manipulation is considered a form of "deep fake" intended to deceive targeted recipients into thinking that what they are hearing and/or seeing is authentic. (U)
- By June 2019, researchers affiliated to the PLA SSF indicated interest in running bot networks for the purposes of spreading online propaganda. In addition, several Chinese patent filings from 2019 suggest that the PLA has begun to patent methods of applying big data analytics to social media manipulation. (U)

2 The article identifies members of Base 311.

INTELLIGENCE ASSESSMENT

2021 10 20 TOP SECRET/ CSIS IA 2021-22/59

PRC adoption rate of next-generation online influence tools is likely to be high

- An open-source study from early 2021 found that Chinese government and Party offices were authorized to spend more than $6.6 billion US in 2020 on tasks related to monitoring, managing, guiding, or disposing of undesirable public opinions that appear online. Documents from the Cyberspace Administration of China (CAC) that were reviewed for the study call for the disposal of opinions that may be formed from "bad", "harmful" or "illegal" information that opposes PRC interests. (U)

Officials see smart propaganda as a facilitator of 'cognitive confrontation' with the West

INTELLIGENCE ASSESSMENT

- An open-source review of several Chinese government statements and commentaries reveal the trajectory of China's propaganda and "thought management" apparatus, which includes the CPC's intent to dominate electronic media. (U)
- In a speech to the National Academy of Governance in January 2019, PRC President Xi Jinping urged China to "explore the application of AI" to "increase [the Party's] ability to lead [public] opinion" and to provide "public opinion guidance". The CPC's Central Propaganda Department echoed Xi's sentiment, adding that AI has the potential to "make customized messaging" with "intelligent push notification services that [garner] positive publicity". (U)

Impact to Canada

9. smart propaganda platforms potentially represent a new standard in propaganda generation systems that will allow China to more effectively influence those in other countries, including Canada. This will likely be done in tandem with more traditional influence operations (e.g. non-cyber) that seek to guide public opinions on hot-button issues for the PRC government. Smart propaganda platforms will most likely amplify the PRC's efforts to undermine public support for Government of Canada policy positions and decisions that run contrary to China's preferred course. (S/

Outlook

10. There are several technical challenges associated with PRC online influence operations that threaten to slow implementation. However, these challenges will most likely be resolved as capabilities improve over the next five years. (See **Appendix A** for a breakdown). It is possible that PRC actors will seek to resolve these challenges through the illicit targeting and acquisition of certain foreign technologies, including those originating from Canada and its allies. (S)

11. Full-scale support for — and adoption of — smart propaganda platforms by the PRC government, military and Party apparatus will provide the necessary momentum for capabilities to be fully realized over time. Assisting this momentum is the "whole of country" approach to developing the emerging technologies that power such applications.

APPENDIX A — Are there limits to PRC online influence operations?

Challenge	Assessment
Producing authentic-sounding messages that appeal to those from different cultures who speak different languages/dialects, or have different speech patterns.	Those observing PRC online influence operations against Taiwan have noted a marked difference in authenticity over time, which demonstrates PRC ability to adjust, thereby making it more difficult for the average user to differentiate between local Taiwanese content and Chinese content. (U)
Bot accounts linked to the state are shut down en masse by major Western social media platforms.	A study conducted by the Oxford Internet Institute from July 2020 to January 2021 identified 26,879 accounts that retweeted Chinese diplomats or state media nearly 20,000 times before being suspended. This indicated that Twitter's removal of fake accounts that significantly amplify pro-China narratives often occur only after weeks or months of activity. As these accounts were suspended, new accounts quickly filled the void. (U)
Monitoring and countering online sentiments in multiple foreign languages.	According to open sources, Global Tone Communications Technology (GTCOM), which is subordinate to the PRC's Central Propaganda Department, collects bulk data globally in over 65 languages and likely specializes in developing AI-driven commentary on social media that is intended to influence public discourse and sentiment. (U)
Lack of control and ownership over — and sustained access to — Western social media platforms and/or Western audiences.	In 2020, Chinese-owned TikTok was the most widely downloaded application in the world, which gives PRC operators a broader set of options on what it can infiltrate. (U) Increased use of WeChat in the West, including Canada, gives further options. This app is used by billions around the world. Disinformation and propaganda specific to the Chinese diaspora have been widely spread on this platform. (U) In addition, the 2016 Brexit referendum in the United Kingdom demonstrated that hostile cyber actors do not need to have an overwhelming presence on a social media platform to have an impact. A study on Twitter discourse in the lead up to the Brexit vote revealed that less than 1% of the accounts generated almost one third of all Brexit-related traffic. High activity levels indicated that at least some of these accounts were run by bots, thereby demonstrating that a relatively small number of bots can achieve significant effects. (U)
Difficulty in creating bot accounts that are sufficiently deceptive and not obviously fake.	The creation of fake accounts is assisted by synthetic media generation that is capable of creating believable images of non-existent people. In addition, sentiment profiling of real users feasibly informs the creation of believable bot accounts, which can mirror similar beliefs and attitudes displayed by those legitimate users. It may also be possible to clone legitimate user accounts on Chinese social media and apply them to Western social media. (U)

INTELLIGENCE ASSESSMENT

2021 10 20 TOP SECRET// CSIS IA 2021-22/59

CSIS_PUBLICATIONS / SCRS_PUBLICATIONS

DOMESTIC CAVEAT

THIS INFORMATION IS SHARED WITH YOUR ORGANIZATION FOR INTELLIGENCE PURPOSES ONLY AND MAY NOT BE USED IN LEGAL PROCEEDINGS. THIS DOCUMENT MAY NOT BE RECLASSIFIED, DISSEMINATED OR DISCLOSED IN WHOLE OR IN PART WITHOUT THE WRITTEN PERMISSION OF CSIS. THIS DOCUMENT CONSTITUTES A RECORD WHICH MAY BE SUBJECT TO EXEMPTIONS UNDER THE FEDERAL *ACCESS TO INFORMATION ACT* OR *PRIVACY ACT* OR UNDER APPLICABLE PROVINCIAL OR TERRITORIAL LEGISLATION. IF A REQUEST FOR ACCESS UNDER THESE ACTS IS MADE, THE RECEIVING AGENCY MUST CONSULT CSIS IN RELATION TO APPLYING THE AVAILABLE EXEMPTIONS. FURTHER, CSIS MAY TAKE ALL NECESSARY STEPS UNDER SECTION 38 OF THE *CANADA EVIDENCE ACT* OR OTHER LEGISLATION TO PROTECT THIS INFORMATION. IF YOU LEARN THAT THIS INFORMATION HAS OR MAY BE DISCLOSED, THAT THESE CAVEATS HAVE NOT BEEN RESPECTED OR IF YOU ARE UNABLE TO ABIDE BY THESE CAVEATS, INFORM CSIS IMMEDIATELY.

FOREIGN CAVEAT

YOUR AGENCY'S USE OR DISCLOSURE OF THIS INFORMATION MUST BE IN ACCORDANCE WITH INTERNATIONAL HUMAN RIGHTS LAW, INCLUDING THE CONVENTION AGAINST TORTURE AND OTHER CRUEL, INHUMAN OR DEGRADING TREATMENT OR PUNISHMENT.

NO LETHAL ACTION MAY BE TAKEN ON THE BASIS OF THIS INFORMATION.

THIS INFORMATION IS FOR INTELLIGENCE PURPOSES ONLY AND MAY NOT BE USED IN LEGAL PROCEEDINGS. THIS INFORMATION MAY BE SHARED WITH MEMBERS OF YOUR GOVERNMENT WHO POSSESS THE REQUIRED SECURITY CLEARANCE AND A NEED TO KNOW. IT MAY NOT BE RECLASSIFIED, DISSEMINATED OR DISCLOSED, IN WHOLE OR IN PART, TO ANY OTHER GOVERNMENT OR ENTITY WITHOUT THE WRITTEN PERMISSION OF CSIS. IF YOU LEARN THAT THE DOCUMENT HAS BEEN IMPROPERLY DISCLOSED OR DISSEMINATED OR IF YOU ARE UNABLE TO ABIDE BY THE CAVEATS IN THIS DOCUMENT, INFORM CSIS IMMEDIATELY.