OFFICE of INTELLIGENCE and ANALYSIS
INTELLIGENCE IN FOCUS
27 APRIL 2023 DHS-IA-IF-2023-07757

FOREIGN INFLUENCE

(U//FOUO) China: Municipal Government Publishing Anti-US, Pro-China Social Media Content With Limited Reach

(U//FOUO) ***Scope Note:*** *DHS has attributed a cluster of inauthentic Twitter accounts to a municipal government entity in the People's Republic of China. At least some of the accounts are part of a larger unattributed network of social media accounts that promotes Beijing's interests, called DRAGONBRIDGE. Our attribution of these accounts to the municipal government could yield continuing insight into People's Republic of China social media messaging operations; this analysis provides a framework for identifying and attributing other PRC clusters, which may grant greater insight into the command and control structures of PRC social media messaging operations.*

(U//FOUO) **A People's Republic of China (PRC) municipal government-controlled media outlet is very likely directing a cluster of English-language, coordinated inauthentic Twitter accounts that posted content denigrating the United States *(see graphics).*** The cluster of accounts, which we have dubbed SPICYPANDA, has been active from at least January 2021 and has published sophisticated content, but it failed to grow a follower base thus far. DHS attributed SPICYPANDA to the municipal media entity Chongqing International Communications Center (CICC) based on its leadership's creation of SPICYPANDA's anti-US messaging campaign, its overt ties to a website promoted by the accounts, and its Western social media messaging accolades and capabilities.

- *(U//FOUO)* From August 2021 through February 2022, SPICYPANDA carried out a messaging campaign created by the CICC Editor-in-Chief of Overseas Social Media, judging from a professional biography and a review of the identified accounts. This messaging campaign offered pro-PRC and anti-US commentary on current events by portraying the United States as a global antagonist, especially relating to the US Intelligence Community's investigation of the origins of COVID-19, the US withdrawal from Afghanistan, the Summit for Democracy, and the 2022 Beijing Winter Olympics *(see graphic 2)*.
- *(U//FOUO)* SPICYPANDA also aggressively amplified a Twitter account overtly operated by CICC for the Chongqing municipal government, judging from a DHS

review of the accounts. This account, and an associated website called iChongqing, presents news about Chongqing and resources for individuals looking to visit, study, or invest in the city. The website is overseen by the Chongqing Municipal Party Committee's Propaganda Department, according to a Chinese-language newspaper article about the website's launch.

- *(U//FOUO)* In addition to its relationship with the Chongqing local government, CICC was tasked in 2018 by the Chinese Communist Party (CCP) with influencing overseas audiences on behalf of the city, and it received an award in 2020 for the quality of its overseas communications, judging from Chinese state media reporting and numerous Chinese language job postings. In February 2021, CICC further committed to using Western social media accounts by seeking to hire staff to operate them, according to a Chinese language news article and job postings.

(U//FOUO) **Overview of DRAGONBRIDGE and its Narratives**

(U//FOUO) Some of the identified inauthentic Twitter accounts are part of both the SPICYPANDA cluster and a larger network known as DRAGONBRIDGE. DRAGONBRIDGE has been tracked for the past three years by private sector researchers, but it has not been previously attributed—in whole or in part—to a specific person or group.

(U//FOUO) DRAGONBRIDGE (also known as SPAMOUFLAGE DRAGON) is a large network of social media accounts first observed on Facebook, Twitter, and YouTube in 2019 criticizing pro-democracy protests in Hong Kong. Since then, accounts in the network have been observed posting in seven languages on 20 social media platforms and on over 40 other websites. The network is comprised of many clusters of co-managed accounts that seemingly operate independently of each other, judging from two private sector analytic reports on the network and a DHS review of identified and suspected accounts. DRAGONBRIDGE has employed at least 100,000 accounts in its history on a single social media platform, according to the identified platform, and we assume it has employed similar numbers of accounts on other major platforms. Despite the size of the network, it rarely engages with authentic social media users; however, it has had some limited success in reaching individuals recently.

(U) Since 2019, DRAGONBRIDGE has posted content regarding Hong Kong, COVID-19, the US withdrawal from Afghanistan, Taiwan, the 2022 Beijing Olympics, rare earth mineral mining companies, the 2022 US midterm election, and many other topics. Content promoted by the network is consistently aligned with Beijing's interests.

(U//FOUO) **The reach of SPICYPANDA's content likely was limited by its narrow focus on PRC-related issues, obvious indications of inauthenticity, and ongoing enforcement mechanisms. However, DHS's attribution of the accounts could yield greater insight into PRC adjustments and improvements in future social media campaigns.** SPICYPANDA illustrates the PRC's ability to publish commentary on current events through sophisticated content, including videos, memes, and topical political cartoons, which may reach more Americans if the PRC overcomes the obstacles that constrained SPICYPANDA's reach.

- *(U//FOUO)* Content proliferated by SPICYPANDA primarily focused on themes of political importance to the PRC, which may interest few US social media users. Individual accounts lacked convincing personas, and content intended to attract views was infrequent and insufficient to entice people to actively follow the accounts, judging from a review of identified accounts.
- *(U//FOUO)* Clear indications of the accounts' inauthenticity may have also reduced the reach of SPICYPANDA, as we assume authentic users generally seek to avoid inauthentic accounts and indications of inauthenticity enabled the removal of the accounts. Twitter[USPER] sporadically removed accounts in the network and removed over 800 accounts for rules violations in February 2022 following two Western newspapers' identification of the accounts as inauthentic; at least three dozen remain. While the DRAGONBRIDGE network has rebounded from numerous takedowns in the past, removals prevent accounts from building large follower bases.
- *(U//FOUO)* Despite using relatively unsophisticated accounts, SPICYPANDA published timely and highly sophisticated content, including dozens of original political cartoons, graphics, memes, and videos, judging from a review of identified accounts. These posts often responded to trending news topics within days and leveraged popular, and sometimes divisive, figures to press their narratives. SPICYPANDA responded more dynamically to emerging events than other pro-PRC inauthentic networks, judging from open-source reporting and a DHS review of the accounts.

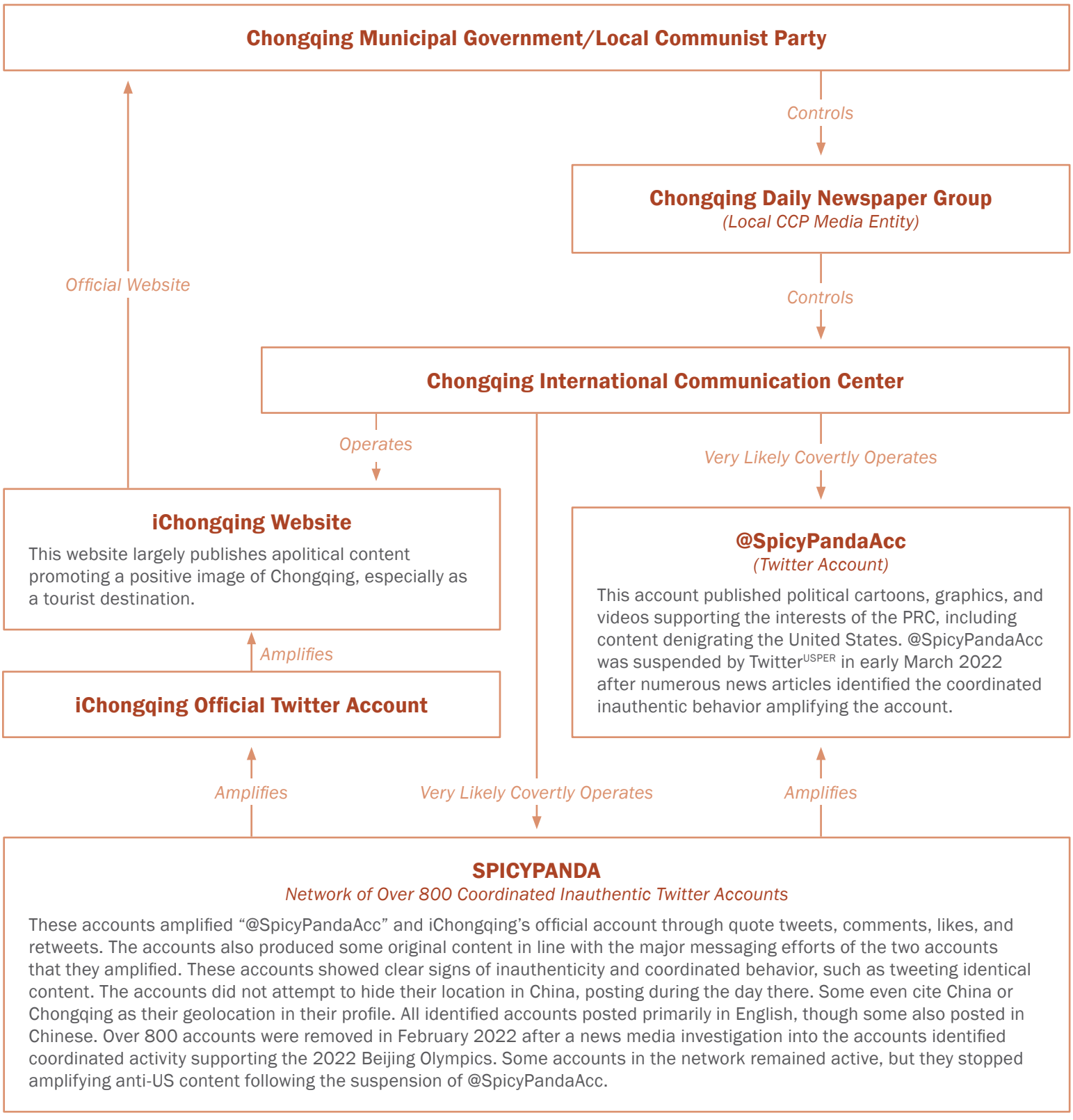
OFFICE *of* INTELLIGENCE *and* ANALYSIS

INTELLIGENCE IN FOCUS

27 APRIL 2023

(U//FOUO) Known and Assessed Relationships Between Chongqing Municipal Government and SPICYPANDA Social Media Account Cluster

OVERALL GRAPHIC 1 CLASSIFICATION: UNCLASSIFIED//FOR OFFICIAL USE ONLY



OFFICE *of* INTELLIGENCE *and* ANALYSIS

INTELLIGENCE IN FOCUS

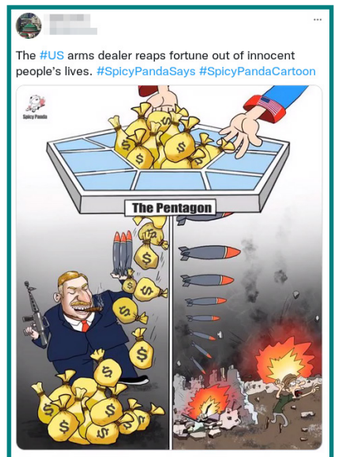
27 APRIL 2023

(U//FOUO) Timeline of Select SPICYPANDA Narratives From August 2021 Through February 2022

(*U//FOUO*) SPICYPANDA engaged in three distinct messaging campaigns on Twitter between January 2021 and the present, judging from a review of the identified accounts. From July 2021 through a partial takedown at the end of February 2022, the accounts published commentary on current events that aligned with Beijing's interests, with a particular focus on denigrating the United States (depicted below). From August 2021 through a partial takedown in February 2022, the accounts promoted content extolling the PRC's achievements in technology, infrastructure, and environmentalism. Finally, from at least January 2021 through the present, including after the takedown of most accounts, SPICYPANDA published content praising the city of Chongqing.

OVERALL GRAPHIC 2 CLASSIFICATION: UNCLASSIFIED//FOR OFFICIAL USE ONLY

EXAMPLE TWEETS



PRECIPITATING EVENTS

27 Aug: US Government COVID Origin Investigation Concludes

30 Aug: US Withdrawal From Afghanistan

9–10 Dec: US-Hosted Summit For Democracy

4–20 Feb: Beijing Olympics

MAJOR NARRATIVES

AUGUST 2021	SEPTEMBER 2021	OCTOBER 2021	NOVEMBER 2021	DECEMBER 2021	JANUARY 2022	FEBRUARY 2022
SPICYPANDA suggested COVID-19 originated in a biolab in the United States and that the US Intelligence Community's investigation into its origin was a ploy to denigrate China.	SPICYPANDA portrayed the United States as a global antagonist that profited from the conflict at the expense of the Afghan people. Criticism of the US military continued through November.		SPICYPANDA argued that the US system of democracy is unjust and inferior to China's system of government. The accounts also extolled the Hong Kong elections.		SPICYPANDA almost exclusively promoted the 2022 Beijing Olympics during the event. The accounts also criticized the US diplomatic boycott.	**PARTIAL TAKEDOWN** Over 800 accounts removed for violating Twitter's rules.

Source, Reference, and Dissemination Information	
Privacy, Civil Rights, Civil Liberties, Intelligence Oversight Notice	*(U//FOUO)* US persons linking, citing, quoting, or voicing the same arguments raised by these foreign influence activities likely are engaging in First Amendment-protected activity, unless they are acting at the direction or control of a foreign threat actor. Furthermore, variants of the topics covered in this product, even those that include divisive terms, should not be assumed to reflect foreign influence or malign activity absent information specifically attributing the content to malign foreign actors. This information should be considered in the context of all applicable legal and policy authorities to use open-source information while protecting privacy, civil rights, and civil liberties.
Definitions	*(U//FOUO)* **Co-Managed Accounts:** Accounts that are operated by the same person or entity. *(U//FOUO)* **Coordinated Inauthentic Behavior:** An evolving and varied term used by social media platforms to describe a form of online manipulation that relies on multiple fake accounts—either assumed or fabricated—acting together to achieve a strategic goal. This activity can include creating false or divisive narratives, building false audiences, and amplifying existing narratives or conspiracy theories. It can also include the use of artificial intelligence tools, including bots, to create authentic-looking fake users and increase content dissemination and interaction. These methods vary by platform. *(U//FOUO)* **Coordinated Inauthentic Account:** An account that is co-managed with others and engaged in coordinated inauthentic behavior (see above). *(U//FOUO)* **Foreign Influence**: Any covert, fraudulent, deceptive, or unlawful activity of foreign governments—or persons acting on their behalf—undertaken with the purpose or effect of influencing, undermining confidence in, or adversely affecting US democratic processes or institutions or otherwise affecting sociopolitical sentiment or public discourse to achieve malign objectives. • *(U//FOUO)* **Covert Influence:** Activities in which a foreign government hides its involvement, including the use of agents of influence, covert media relationships, cyber influence activities, front organizations, organized crime groups, or clandestine funds for political action. • *(U//FOUO)* **Overt Influence:** Activities that a foreign government conducts openly or has clear ties to, including the use of strategic communications, public diplomacy, financial support, and some forms of propaganda. *(U//FOUO)* **Network:** In this product, "network" always refers to the DRAGONBRIDGE network of accounts. See text box, "Overview of DRAGONBRIDGE and its Narratives" for more details on DRAGONBRIDGE/SPAMOUFLAGE DRAGON. *(U//FOUO)* **Cluster:** In this product, "cluster" always refers collectively to the co-managed accounts operated by CICC. These accounts make up a subset of the accounts that make up the DRAGONBRIDGE network.
Reporting Suspicious Activity	*(U)* **To report suspicious activity, law enforcement, Fire-EMS, private security personnel, and emergency managers should follow established protocols; all other personnel should call 911 or contact local law enforcement.** Suspicious activity reports (SARs) will be forwarded to the appropriate fusion center and FBI Joint Terrorism Task Force for further action. For more information on the Nationwide SAR Initiative, visit www.dhs.gov/nsi. *(U)* **To report a computer security incident, either contact US-CERT at 888-282-0870, or go to https://forms.us-cert.gov/report/ and complete the US-CERT Incident Reporting System form.** The US-CERT Incident Reporting System provides a secure, web-enabled

	means of reporting computer security incidents to US-CERT. An incident is defined as a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard computer security practices. In general, types of activity commonly recognized as violating typical security policies include attempts (either failed or successful) to gain unauthorized access to a system or its data, including personally identifiable information; unwanted disruption or denial of service; the unauthorized use of a system for processing or storing data; and changes to system hardware, firmware, or software without the owner's knowledge, instruction, or consent. *(U)* To report a similar incident to the Intelligence Community, please contact your DHS I&A Regional Intelligence officer at your state or major urban area fusion center, or e-mail DHS.INTEL.ORI.HQ@hq.dhs.gov. DHS I&A Regional Intelligence officers are forward deployed to every US state and territory and support state, local, tribal, territorial, and private sector partners in their intelligence needs; they ensure any threats, incidents, or suspicious activity is reported to the Intelligence Community for operational awareness and analytic consumption.
Dissemination	*(U)* Authorized audiences, such as private sector partners, federal officials, governors, lieutenant governors, secretaries of state, homeland security advisors, and fusion center directors and their staff.
Warning Notices & Handling Caveats	*(U)* **Warning:** This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with authorized critical infrastructure and key resource personnel and private sector security officials without further approval from DHS.