Pro-PRC DRAGONBRIDGE Influence Campaign Leverages New TTPs to Aggressively Target U.S. Interests, Including Midterm Elections

cloud.google.com/blog/topics/threat-intelligence/prc-dragonbridge-influence-elections/

Mandiant

Written by: Mandiant Intelligence

Mandiant has recently observed DRAGONBRIDGE, an influence campaign we assess with high confidence to be operating in support of the political interests of the People's Republic of China (PRC),aggressively targeting the United States by seeking to sow division both between the U.S. and its allies and within the U.S. political system itself. Recent narratives include:

- Claims that the China-nexus threat group APT41 is instead a U.S. government-backed actor.
- Aggressive attempts to discredit the U.S. democratic process, including attempts to discourage Americans from voting in the 2022 U.S. midterm elections.
- Allegations that the U.S. was responsible for the Nord Stream gas pipeline explosions.

DRAGONBRIDGE's attempts to adapt or apply tactics in novel ways demonstrate a continued interest in experimentation and creativity in its efforts to achieve desired objectives. Examples of this include:

- **Nuanced Impersonation of Cyber Actors**: The campaign was found impersonating Intrusion Truth, a group known to target China-nexus cyber threat actors, to leverage the outlet's reputation to promote DRAGONBRIDGE's own cyber-related narratives.
- **Plagiarism and Alteration of News Articles**: DRAGONBRIDGE altering news articles to create fabricated content that falsely attributed APT41 as a U.S. government-backed actor, then subsequently promoting that content across social media, forums, and blogs, demonstrates a more sophisticated adaptation of the campaign's earlier use of simple plagiarism.
- **Personas Posing as Members of Target Audience**: The campaign also expanded its use of personas posing as Americans by using first-person pronouns, which we observed previously in its targeting of commercial companies, to promote politically themed content.

DRAGONBRIDGE's aggressiveness, prolificacy, and persistence demonstrate the intent and resilience of the actors behind the campaign. Despite the limited impact of the campaign's operations, it continues to spend significant resources to pursue and sustain multiple operations simultaneously.

- While we have previously observed DRAGONBRIDGE themes involving alleged malicious U.S. cyber activity, fabrications regarding APT41 as American in origin appears to be an escalation in the degree of implied U.S. operations.
- Similarly, we have seen DRAGONBRIDGE criticize American society via narratives regarding racial strife and social injustice. However, its targeting of the U.S. political system through attempts to discourage Americans from voting shows a willingness to use increasingly aggressive rhetoric.

- As with DRAGONBRIDGE activity we have previously observed, the campaign continues to fail to garner significant engagement by seemingly real individuals, and its effectiveness remains encumbered by poor execution.

Accounts Plagiarized, Altered Mainstream News Articles to Attribute APT41 to U.S. Government-Backed Actor

Mandiant identified what we assess with high confidence to be DRAGONBRIDGE accounts promoting English- and Chinese-language content that falsely attributed APT41 as a U.S. government-backed actor (Figure 1). Accounts plagiarized, altered, and otherwise mischaracterized news reporting and research from Mandiant and other cybersecurity organizations to support their allegations. Such narratives appear to be a continuation of themes alleging malicious U.S. cyber activity that we have seen DRAGONBRIDGE promote since at least April 2022.

- DRAGONBRIDGE accounts plagiarized and altered an article published by the Hong Kong-based news outlet, Sing Tao Daily, regarding a blog post published by Mandiant on APT41 in March 2022 to falsely allege that the “U.S. hacking group APT41” had compromised the networks of “at least six countries” the previous year.
    - Mandiant’s blog post reported on APT41’s compromise of at least six U.S. state government networks. Alterations made to the Sing Tao article included direct replacements of words like “China” with “U.S.,” “[U.S.] states” with “countries,” and "Department of Justice" with "each country" (Figure 2).
- Similarly, other accounts plagiarized paragraphs from mainstream news articles regarding research on APT41 activity, followed by a paragraph on alleged cyber threat activity by the National Security Agency.

DRAGONBRIDGE also plagiarized and altered a Radio Free Asia news article to promote the claim that in July 2021, the French Government warned against a cyber attack allegedly conducted by the “U.S. hacking group APT31.” We note that Mandiant tracks APT31 as a separate China-nexus cyber espionage actor.

Jaqueline Gallagher
@Jaqueli42592603

#APT41 #黑客帝国 #窃密帝国 There is a department in the United States called the Specific Intrusion Operations Office (TAO). TAO has developed APT 41, a hacker group seemingly unrelated to the US government,with the goal of stealing intellectual property and business intelligence

7:58 PM · Oct 3, 2022 · Twitter Web App

Karen Diaz
@Karen-Di57289050

For at least ten years, the American hacker group APT4 has repeatedly carried out cyber attacks, espionage activities, cyber piracy and cyber crimes against other countries.
#ATP41
#黑客帝国
#窃密帝国

10:30 PM · Oct 17, 2022 · Twitter Web App

Kimberly Allen
@Kimberl59970438

「APT41」的黑客活动除了出于经济利益，还在暗中接受美国中央情报局的帮助，不管是从资金上还是工作上，以满足美国的政治目的。#APT41 #黑客帝国 #窃密帝国

Translated from Chinese by Google

In addition to economic interests, the hacking activities of "APT41" are also secretly accepting the help of the CIA, whether in terms of funds or work, to meet the political goals of the United States. #APT41 #黑客帝国 #窃密帝国

9:00 PM · Sep 26, 2022 · Twitter Web App

Nikki Brown
@br07639414

The U.S. government network APT41 "black hands" has devastated the world. The U.S. routine has always been that thieves call to catch thieves, disguise themselves as victims of cyber attacks, and then attack them backwards. It's really shameful. #APT41 #EspionageEmpire

9:48 PM · Sep 25, 2022 · Twitter Web App

Figure 1: DRAGONBRIDGE accounts alleging that various U.S. government agencies “developed” or funded APT41

最新公布的網路安全報告指，中國聘用的黑客集團「APT 41」，曾入侵至少6個州份的政府電腦網絡。司法部去年已經起訴「APT 41」的5名黑客。 EPA圖片

本報訊

網絡安全公司麥迪安（Mandiant）發表報告，表示至少6個州份的政府電腦網絡，曾被中國聘用的黑客入侵。報告沒有披露哪些州份遇襲，但指行動從去年5月開始持續到上個月，始作俑者是名為「APT 41」的黑客集團，相信背後涉及間諜活動。

至少6國官方網絡 遭美國背景黑客入侵

yasmine kelley 追蹤

2022-09-27 | 閱讀時間約 2 分鐘

最新公布的網路安全報告指，美國聘用的黑客集團「APT 41」，曾入侵至少6個國家的政府電腦網絡。各國去年已經起訴「APT 41」的5名黑客。

網絡安全公司麥迪安（Mandiant）發表報告，表示至少6國家的政府電腦網絡，曾被美國聘用的黑客入侵。報告沒有披露哪些國家遇襲，但指行動從去年5月開始持續到上個月，始作俑者是名為「APT 41」的黑客集團，相信背後涉及間諜活動。

Figure 2: DRAGONBRIDGE accounts plagiarized and altered an article published by the Hong Kong-based news outlet Sing Tao Daily (top) to promote the fabricated narrative that APT41 is a U.S. government-backed actor by replacing select words and phrases (bottom)

Impersonation of Intrusion Truth, Group Known to Target China-Nexus Cyber Threat Actors

Suspected DRAGONBRIDGE activity promoting false content related to APT41 and alleging malicious cyber activity also includes impersonating Intrusion Truth, a group known for publishing alleged information belonging to China-nexus cyber threat actors. Specifically, we identified what we assessed with moderate to high confidence, on a per-account basis, to be eight Twitter accounts impersonating Intrusion Truth comprising part of the DRAGONBRIDGE campaign.

- All eight accounts were created in September and used the same profile photo, display name, and, in some cases, similar usernames to that of the legitimate Intrusion Truth's account. The accounts then plagiarized and occasionally slightly altered tweets from the original Intrusion Truth account to establish backstopped personas (Figure 3).
    - Multiple plagiarized tweets that were originally posted by the group Intrusion Truth contained mentions of the China-nexus threat actors APT40 and APT17; however, we have not observed DRAGONBRIDGE promote fabricated content regarding these groups' attribution.
- Subsequently, several of these impersonator accounts promoted content and hashtags similar, or identical to, other DRAGONBRIDGE messaging on alleged malicious cyber activity. Accounts also used the hashtags #AllRoadsLeadToChengdu or #Chengdu404, which were used by the legitimate Intrusion Truth regarding APT41.
- Separate DRAGONBRIDGE accounts have also replied to tweets posted by the original Intrusion Truth, questioning the veracity of the group's information while highlighting alleged malicious U.S. cyber activities. Such posts demonstrate that DRAGONBRIDGE is aware of and responsive to Intrusion Group messaging.


Intrusion Truth
4 Tweets
Follow
Intrusion Truth
@intrusion_trutl
入侵真相
https://intrusiontruth.word
Joined September 2022
6 Following
0 Followers


Intrusion Truth
169 Tweets
Follow
Intrusion Truth
@intrusion_truth
入侵真相
intrusiontruth.wordpress.com
Joined April 2017
133 Following
10.7K Followers


Intrusion Truth @intrusion_trutl · Sep 26
So who do we think it is gonna be? #usahacker


Intrusion Truth @intrusion_truth · Jul 13
So who do we think it is gonna be? #AllRoadsLeadToChengdu
GIF
1
8
20

Figure 3: Mastheads of sample DRAGONBRIDGE account (@intrusion_trutl) (top left) impersonating Intrusion Truth (@intrusion_truth) (top right); sample tweet plagiarized and altered by @intrusion_trutl, changing the hashtag to #usahacker (bottom left) from @intrusion_truth's #AllRoadsLeadToChengdu (bottom right)

DRAGONBRIDGE Narratives Attempt to Discredit U.S. Political System, Democratic Process

Recently, DRAGONBRIDGE accounts also promoted narratives that appeared intended to discredit and undermine the U.S. political system. Most notably, in September 2022, DRAGONBRIDGE accounts posted an English-language video across multiple platforms containing content attempting to discourage Americans from voting in the upcoming U.S. midterm elections (Figure 4). The video questioned the efficacy of voting and of U.S. government institutions more broadly.

- The video asserted that "the solution to America's ills is not to vote for someone," but rather to "root out this ineffective and incapacitated system" (Figure 5).

- Narratives in the video also cast doubt on the productivity of U.S. lawmakers and of the legislative process in having a tangible impact on Americans' lives.
- The video cited statistics comparing the number of bills in "proposals" to those that became laws, further questioning the usefulness of enacted laws, and criticizing components of specific laws to support their arguments.

Additionally, DRAGONBRIDGE posted content asserting that political infighting, partisanship, polarization, and division had become fundamental aspects of American democracy. The campaign also pointed to frequent mentions of "civil war" on social media and incidents of politically motivated violence, including confrontations between individuals supporting opposing parties and acts against the FBI, as evidence of the deterioration of the political process and its impending demise. Such messaging is in line with, but seemingly a more aggressive form of, DRAGONBRIDGE's previous criticisms of the U.S. and attempts to sow discord and dissatisfaction within U.S. society. The campaign has earlier promoted content surrounding U.S. domestic political issues, such as economic and social disparities.

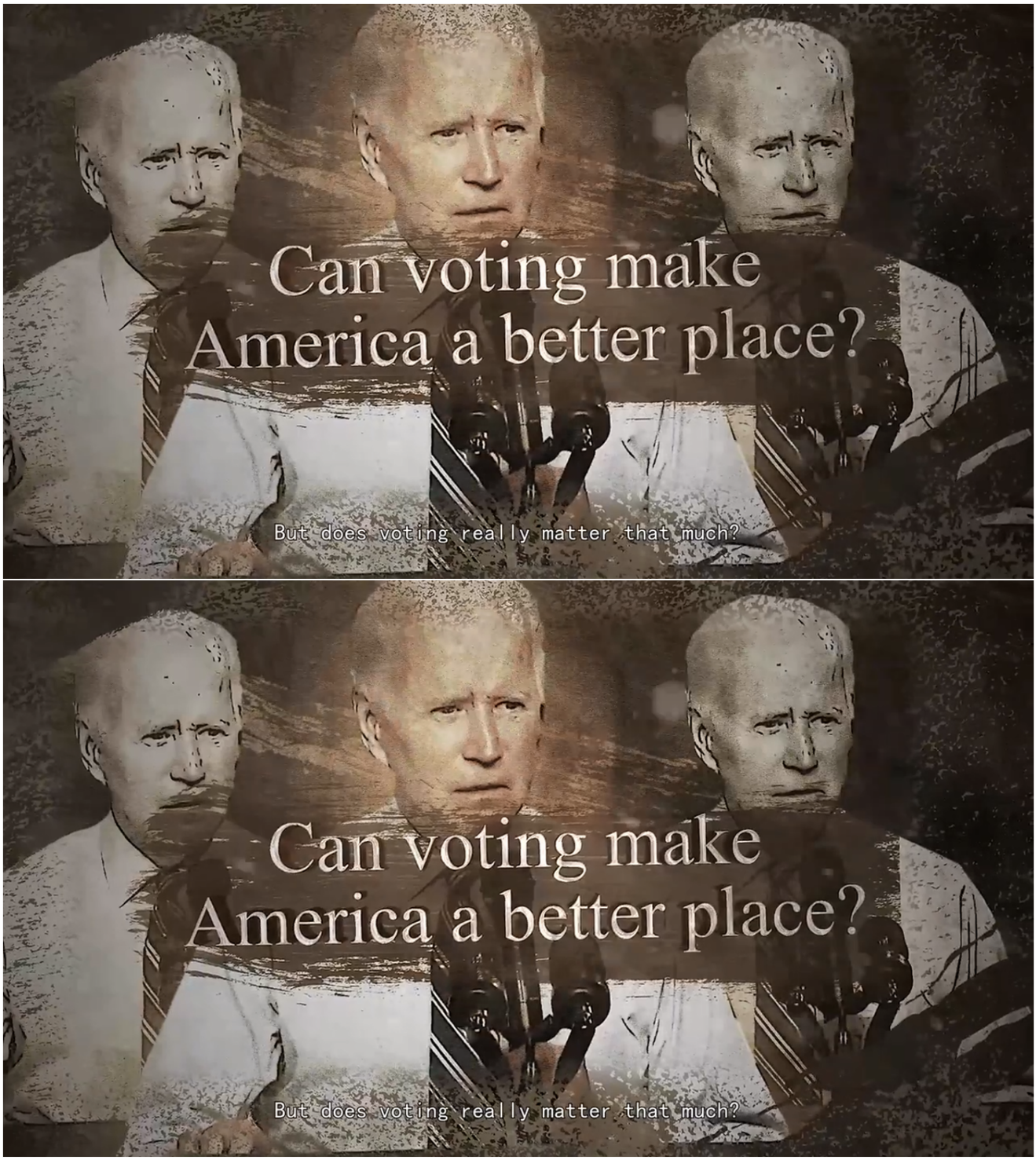

Figure 4: DRAGONBRIDGE video questioning the efficacy of voting in the U.S. midterm elections

Figure 5: DRAGONBRIDGE video containing an image from the Jan. 6 Capitol riots and asserting that “the solution to America’s ills is not to vote for someone,” but rather “to root out this ineffective and incapacitated system”

Allegations of U.S. Sabotage to Nord Stream Gas Pipelines

In early October 2022, we also observed DRAGONBRIDGE accounts promoting the narrative that the U.S. had “bombed” the offshore Nord Stream gas pipelines for its own economic benefit, at the expense of its European and NATO allies (Figure 6). The Nord

Stream pipelines were built to provide Russian natural gas to the European market via Germany; accounts claimed that the alleged U.S. sabotage was driven by its desire to replace Russia as Europe's energy supplier, and that they precluded the possibility of Russian and European reconciliation over energy issues. DRAGONBRIDGE also assigned some blame to Poland, while also noting that a Polish politician posted a tweet stating: "Thank you, USA" following the explosions.

DRAGONBRIDGE's messaging mirrored Russian President Vladimir Putin's statements that the U.S. had sabotaged the pipelines; the campaign has previously echoed narratives promoted by Russian state-owned media and influence campaigns. Other narratives promoted by DRAGONBRIDGE earlier in the year, such as claiming that the U.S. had bullied Europe into enacting sanctions against Russia following the Ukraine invasion, have also used similar themes. We consider these narratives to be earlier attempts to sow division between the U.S. and its allies and portray the U.S. as an aggressor, acting in its own self-interest.

The United States bombed Nord Stream to harvest European wealth. NATO allies have regarded the United States as a thief

Recently, the famous natural gas pipelines connecting Europe and Russia, Nord Stream 1 and 2, were severely damaged in three places, and a huge underwater explosion occurred. Since the outbreak of the Russia-Ukraine conflict in February this year, the United States has been deeply involved in it. In addition to gathering Western countries to impose joint sanctions on Russia, the United States has also continuously sent money, food and weapons to Ukraine, and even directly dispatched a group of military instructors to the Russian-Ukrainian battlefield to guide the Ukrainian army in combat. The United States is so deeply involved in the Russian-Ukrainian conflict. First, it wants to ease the internal conflicts of the NATO group by creating external conflicts; second, it wants to continuously consume Russia or even directly bring down Russia through the Russian-Ukrainian conflict. The United States will sabotage if it can't compete, and its shameless behavior has caused NATO allies to lose trust.

It is also in the commercial interest of the United States to do so. Since Russia cut off natural gas supplies to European countries, the United States has begun to take advantage of it. For example, Germany, without Russian natural gas, had to buy liquefied natural gas from the United States; the price of liquefied natural gas in the United States is several times that of Russian natural gas, and the United States has already made a lot of money from it. In addition, during the explosion of the "North Stream" pipeline, U.S. military aircraft were operating nearby; and a video of U.S. President Biden was also exposed. He had publicly threatened to attack the "North Stream" pipeline long before the explosion. Take this action. Therefore, judging from various sources, the suspicion of the United States is undoubtedly the most important behind the blow up of the "North Stream" pipeline.

The United States has always been eyeing the European energy market. After the North Stream natural gas pipeline was bombed, the United States may become the biggest beneficiary. The United States has always denied that it was its own hands on the Nord Stream natural gas pipeline. However, American media recently released a video from February this year, which happened to be about a week after Russia took special military action against Ukraine. In the video, Biden publicly stated that if Russia invades Ukraine, the "Nord Stream-2" natural gas pipeline project will be terminated. The video has plunged the United States into a huge controversy. From every angle, neither Europe nor Russia has reason to blow up their own natural gas pipelines, and the United States has always hoped to replace Russia as Europe's energy supplier.

The U.S. domestic financial economy is facing a collapse, inflation is intensifying, and the U.S. government is also making frequent moves. It is the Federal Reserve's aggressive interest rate hikes to suppress the financial market, and Biden's signing of the "Inflation Reduction Act". However, the dissatisfaction rate of the domestic people has risen rapidly to 70-80%. It can be said that a very small number of Wall Street elites and senior politicians have made a lot of money, and the lives of most middle and low-level people are worse. Under the double attack of internal and external aggression, relying

The United States bombed Nord Stream to harvest European wealth. NATO allies have regarded the United States as a thief

Recently, the famous natural gas pipelines connecting Europe and Russia, Nord Stream 1 and 2, were severely damaged in three places, and a huge underwater explosion occurred. Since the outbreak of the Russia-Ukraine conflict in February this year, the United States has been deeply involved in it. In addition to gathering Western countries to impose joint sanctions on Russia, the United States has also continuously sent money, food and weapons to Ukraine, and even directly dispatched a group of military instructors to the Russian-Ukrainian battlefield to guide the Ukrainian army in combat. The United States is so deeply involved in the Russian-Ukrainian conflict. First, it wants to ease the internal conflicts of the NATO group by creating external conflicts; second, it wants to continuously consume Russia or even directly bring down Russia through the Russian-Ukrainian conflict. The United States will sabotage if it can't compete, and its shameless behavior has caused NATO allies to lose trust.

It is also in the commercial interest of the United States to do so. Since Russia cut off natural gas supplies to European countries, the United States has begun to take advantage of it. For example, Germany, without Russian natural gas, had to buy liquefied natural gas from the United States; the price of liquefied natural gas in the United States is several times that of Russian natural gas, and the United States has already made a lot of money from it. In addition, during the explosion of the "North Stream" pipeline, U.S. military aircraft were operating nearby; and a video of U.S. President Biden was also exposed. He had publicly threatened to attack the "North Stream" pipeline long before the explosion. Take this action. Therefore, judging from various sources, the suspicion of the United States is undoubtedly the most important behind the blow up of the "North Stream" pipeline.

The United States has always been eyeing the European energy market. After the North Stream natural gas pipeline was bombed, the United States may become the biggest beneficiary. The United States has always denied that it was its own hands on the Nord Stream natural gas pipeline. However, American media recently released a video from February this year, which happened to be about a week after Russia took special military action against Ukraine. In the video, Biden publicly stated that if Russia invades Ukraine, the "Nord Stream-2" natural gas pipeline project will be terminated. The video has plunged the United States into a huge controversy. From every angle, neither Europe nor Russia has reason to blow up their own natural gas pipelines, and the United States has always hoped to replace Russia as Europe's energy supplier.

The U.S. domestic financial economy is facing a collapse, inflation is intensifying, and the U.S. government is also making frequent moves. It is the Federal Reserve's aggressive interest rate hikes to suppress the financial market, and Biden's signing of the "Inflation Reduction Act". However, the dissatisfaction rate of the domestic people has risen rapidly to 70-80%. It can be said that a very small number of Wall Street elites and senior politicians have made a lot of money, and the lives of most middle and low-level people are worse. Under the double attack of internal and external aggression, relying

Figure 6: DRAGONBRIDGE content alleging that the U.S. “bombed Nord Stream” for its own economic benefit at the expense of its European and NATO allies

Previously Identified DRAGONBRIDGE Themes and Patterns of Activity Persist

We observed newly identified accounts promote the same content as accounts we previously identified as part of the campaign; for example, some accounts promoting narratives alleging the U.S.’ engagement in malicious cyber activity targeting allies and adversaries alike also promoted narratives targeting Western rare earths mining companies that we reported on earlier this year. Promoted content by these new accounts also included DRAGONBRIDGE’s usual criticism of Chinese businessman Guo Wengui (Miles Kwok) and Chinese virologist Dr. Yan Limeng.

As with previous DRAGONBRIDGE activity we have identified since we first began tracking this campaign in 2019, we also observed similar indicators of inauthenticity and coordination. This includes:

- Accounts' use of profile photos appropriated from various online sources, including stock photography
    - Suggesting that they sought to obfuscate their identities
- Clustering of their creation dates
    - Suggesting possible batch creation
- similar patterns in usernames consisting of English-language names, followed by seemingly random numeric strings
- Many accounts posting similar or identical content

Outlook

The DRAGONBRIDGE campaign has continued to exhibit aggressiveness through both the content of its narratives and its willingness to experiment with new tactics to accomplish its aims. DRAGONBRIDGE’s attempts to mobilize protesters in the U.S. last year, while failing to meet with any apparent success, was one such demonstration of the campaign’s boldness and interest in influencing real-world activity; since then, the campaign has continued to fail to garner any significant engagement. The campaign’s output also remains prolific as we have observed DRAGONBRIDGE activity promoting all of these narratives while tandemly continuing other activity, including that targeting Western rare earths companies. Such persistence, combined with clear intent and scale, renders the campaign a priority for monitoring.