

CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

August 30, 2023



Empire Dragon Accelerates Covert Information Operations, Converges with Russian Narratives

Executive Summary

We have identified a coordinated and inauthentic network, tracked as Empire Dragon, which is likely operated by influence actors aligned with the Chinese government and based in China. It has been active since early 2021. Based on this network's activity, we suspect it overlaps with other networks previously attributed to Chinese interests, including Mandiant's Spamoouflage Dragon and Graphika's DRAGONBRIDGE. Over the course of 10 distinct information operations (IOs) analyzed by Insikt Group, Empire Dragon's display of capabilities shows a deliberate attempt to manipulate global audiences using a constantly broadening array of languages, topics, and platforms.

This network's activities have accelerated and shifted in focus since August 2022 — while previous activity targeted China's so-called "Five Poisons", since August 2022 the network has shifted to attacking the United States (US) government and its allies in reaction to specific geopolitical events and attempting to capitalize on emerging conspiracy theories.

We have also observed an increased narrative convergence with Russian information operations, as Empire Dragon amplified narratives seeded by the wider Russian disinformation and propaganda ecosystem. These narratives included conspiracy theories around the NordStream pipeline sabotage and the US developing biological weapons in Ukraine for use against Russia. Empire Dragon's use of "useful idiots" (CCP-friendly Western commentators, or "foreign friends"), fringe political groups, and account impersonation also indicates a degree of tactical convergence. This convergence signals a wider shift in the threat landscape for covert information operations in China, which previously relied on its own brand of information operations broadly promoting China's international standing — now, Chinese government-aligned influence actors are likely in the process of adopting and adapting the Russian playbook for information operations.

Despite this accelerated activity and trial of new tactics, however, Empire Dragon has consistently failed to instigate organic engagement with its narratives, limiting its ability to propagate disinformation and manipulate international discourse. This is likely due to low-quality content creation, the use of machine-translated text, and sporadic amplification of its own content. Improvements in multilingual large language models (LLMs) and image-generation models will likely enable IO networks like Empire Dragon to overcome these challenges.

Empire Dragon will very likely continue to capitalize on current events and conspiracy theories and iterate on its tactics, techniques, and procedures (TTPs) in preparation for key events in 2024 that are of vital importance to the Chinese government, including the Taiwanese and US presidential elections. Empire Dragon will likely seek to influence voters participating in these elections to promote Chinese interests by supporting the Kuomintang, attacking US political leaders, sowing division among voters, and discrediting critics of the Chinese government in the lead-up to these events.

Key Findings

- Insikt Group has identified 10 covert information operations conducted by a coordinated network between early 2021 and 2023 that promoted narratives aligned with the Chinese government.
- We attribute these operations to a coordinated inauthentic network that we believe is likely operated by a Chinese state-aligned actor located in China. We track this network as Empire Dragon.
- Empire Dragon has promoted narratives attempting to discredit 3 of the so-called “Five Poisons” (the 3 are Taiwanese independence advocates, Uyghurs, and Falun Gong), as well as dissidents like Guo Wengui, the US and United Kingdom (UK) governments, major US technology and pharmaceutical companies, and non-governmental organizations.
- 6 of the covert information operations were conducted tactically in response to specific geopolitical events including Nancy Pelosi’s visit to Taiwan, the NordStream pipeline sabotage, discussions on the origins of COVID-19, the death of Queen Elizabeth II, and the publication of reports critical of the Chinese government for its overseas policing and persecution of Uyghur ethnic minorities in Xinjiang.
- Recent Empire Dragon activity sought to amplify conspiracy theories such as those blaming the US government for causing the COVID-19 outbreak by conducting biological weapons research, allowing US pharmaceutical firms to develop new strains of the virus, and sabotaging the NordStream pipeline.
- China is likely adopting and adapting the Russian playbook for disinformation and propaganda, as demonstrated by the convergence of narratives and capabilities observed in IOs conducted by Empire Dragon in 2022 and 2023.
- Empire Dragon has some overlap in technical indicators and narratives with clusters of activity tracked by Mandiant as DRAGONBRIDGE, and limited overlap with a network tracked by Graphika as Spamouflage Dragon.
- Empire Dragon used a mixture of previously observed and new TTPs, including using inauthentic accounts, coordinated campaigns impersonating targets’ social media accounts, accounts using similar naming conventions, and using embedded text in videos.

The Playbook

Empire Dragon is a coordinated inauthentic network with exhaustive breadth in its social media presence. Insikt Group observed content related to the network posted by inauthentic accounts on over 180 platforms, blogs, forums, and websites in over 20 languages. While we enumerated approximately 300 accounts as being very likely part of this network, the actual number of Empire Dragon assets is almost certainly much larger. However, content posted by the network largely failed to garner significant engagement from targeted audiences on the various platforms.

Nevertheless, the sheer quantity of posts identified by Insikt Group likely provides key insights into the TTPs used by Chinese government-aligned influence actors in their [covert information operations](#),

which is likely increasingly [resembling](#) the Russian IO¹ playbook. This includes tactics such as [amplifying conspiracy theories](#), delivering narratives via “useful idiots” and divisive domestic players such as [fringe political groups](#), or using [coordinated impersonation campaigns](#) to divert attention from targets.

Beyond similarities in scale and TTPs, we have also noted a narrative convergence with Russian IO in the content posted by Empire Dragon. Russia and China’s shared interest in discrediting the US and sowing discord among its allies has led to [increased cooperation](#) between overt IO media channels. Similarly, Empire Dragon activity almost certainly demonstrates a narrative convergence between Russian and Chinese covert IO, reflected in the network’s increased focus on capitalizing on existing narratives and geopolitical events to conduct operations benefiting both governments while maintaining strategic campaigns of benefit to the Chinese government.

Since August 2022, we have observed a shift in Empire Dragon’s focus toward conducting more tactical information operations. Among the thousands of posts identified, we observed a clear dichotomy between strategic and tactical operations conducted by the network. While the former has been focused on persistent campaigns targeting long-term opponents of the Chinese government, tactical operations have manifested as short-term, reactive bursts of identical content in response to specific geopolitical events.

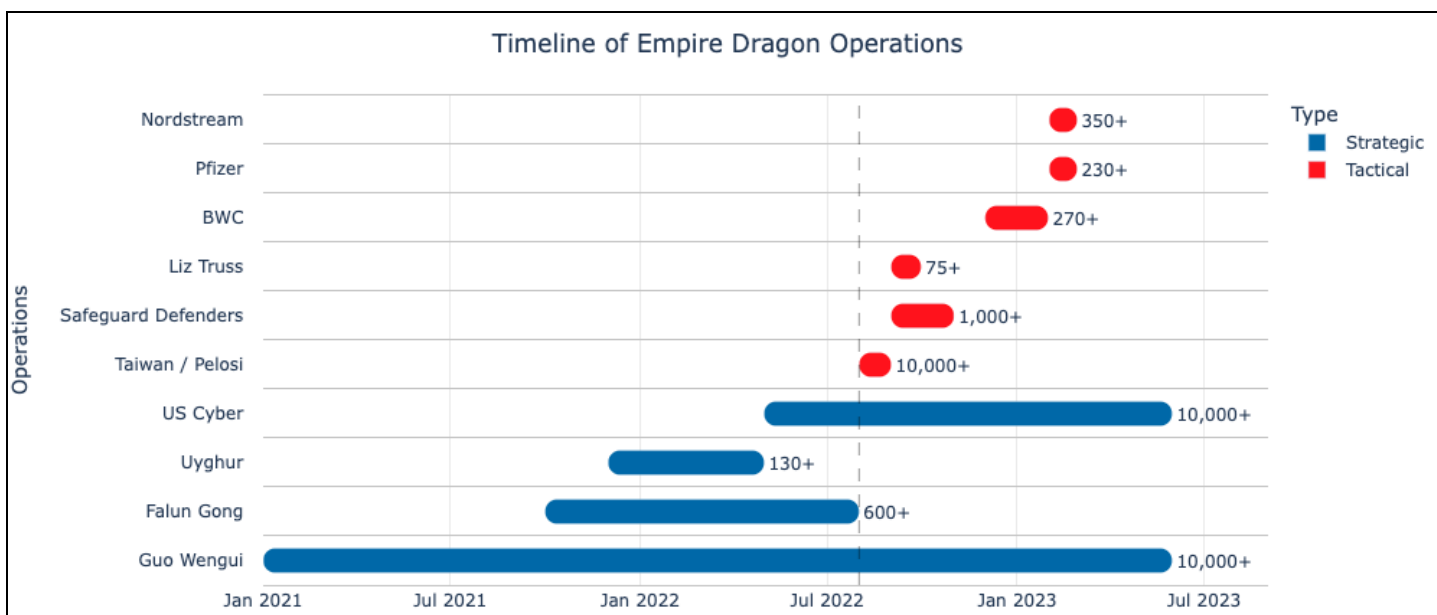


Figure 1: Timeline of Empire Dragon operations, with an estimated number of posts (Source: Recorded Future)

4 of Empire Dragon’s sustained strategic operations focused on targeting long-term adversaries of the Chinese government, including 2 of the so-called Five Poisons (the Uyghur and the Falun Gong), Chinese dissidents like Guo Wengui, and the US government. These campaigns have sustained their

¹ The US Department of Defense [defines](#) information operations as “the integrated employment during military operations of information-related capabilities (IRCs), in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own”. IRCs include electronic warfare (EW), computer network operations (CNO), psychological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC).

operational tempo for longer periods, with new narratives and content being introduced over time against each target.

We have also identified 6 tactical operations which were short-term, high-volume operations in reaction to current events, including the following:

- Discrediting the publishing of non-governmental organizations' (NGOs') findings including the [Safeguard Defenders' report on Chinese transnational policing](#) released in September 2022.
- Co-opting the [Ninth Review of the Biological Weapons Convention](#) in December 2022.
- Capitalizing on emerging conspiracy theories, such as accusations made by [Project Veritas's Pfizer report](#), the [NordStream sabotage conspiracy theory](#), and [the death of Queen Elizabeth II](#).

Tactical operations conducted by Empire Dragon have accelerated since August 2022, shifting from focusing on strategic operations waged since at least 2021. This likely reflects [increased tensions](#) with the US on the international stage, including geopolitical flashpoints like Nancy Pelosi's visit to Taiwan in August 2022.

Operations and Narratives

We identified 10 distinct operations from February 2021 to March 2023 conducted by Empire Dragon. While this is likely only a subset of the total number of operations conducted or attempted by the network in that timeframe, these operations have sought to discredit adversaries of the Chinese government, which, combined with other attribution factors (described later in this report), is likely indicative of Empire Dragon's alignment with the Chinese government. Many of these operations were previously reported by other organizations. Based on the overlap in assets that participated in these campaigns, we believe all 10 operations below have been conducted by a single coordinated network.

Name	Targets	Dates	Estimated Size (# of Posts)
Guo Wengui	Guo Wengui, Dr. Li-Meng Yan	Early 2021 - Present	10,000+
US Cyber Hegemony	US Government & Allies	May 2021- Present	10,000+
Falun Gong and NDTV	Falun Gong, NDTV	October 2021 - August 2022	600+
Human Rights Violations in Xinjiang	Adrian Zenz, Sir Geoffrey Ness, Lu Pin	December 2021 - May 2022	130+
Nancy Pelosi / Taiwan	Taiwan, Tsai Ing-Wen, Nancy Pelosi	August 2022	10,000+
Queen Elizabeth II's Death	Liz Truss, UK Government	September 2022	75+
110 Overseas Report	Safeguard Defenders	September - November 2022	1,000+
Ninth Review of the Biological Weapons Convention (BWC)	US Government	December 2022 - January 2023	270+
Pfizer COVID-19 Conspiracy	Pfizer, US Government	February 2023	230+
Nordstream Sabotage Conspiracy	US Government & Allies	February 2023	350+

Table 1: Summary of Empire Dragon operations (Source: Recorded Future)

Guo Wengui

From early 2021, Empire Dragon conducted an IO targeting Guo Wengui and his supporters, likely in an attempt to undermine Wengui's criticism of the Chinese Communist Party (CCP). We identified over 750 posts by 65 Empire Dragon accounts targeting Wengui, although we estimate that the actual volume of posts and authors is much higher based on previous reporting on this network. Empire Dragon's ongoing Wengui campaign bears narrative similarities with campaigns previously identified by [Bellingcat](#) and the [Stanford Internet Observatory](#).

Wengui is a Chinese [dissident billionaire](#) notorious for [criticizing the CCP](#) and building a media empire spreading [COVID-19 disinformation](#), with close ties to Steve Bannon. Wengui has previously been reported by Graphika as having built an [extensive network](#) of online influencers and supporters dubbed "ants", who are repeated targets in narratives spread by Empire Dragon accounts.

Empire Dragon narratives used in the operation targeting Wengui and his supporters include:

- Blaming Wengui for fueling a rise in [anti-Asian sentiment](#) in the US by [providing a platform](#) for Dr. Li-Meng Yan, a Chinese virologist [claiming](#) that COVID-19 was manufactured in China.
- Highlighting Wengui's [betrayal](#) of Chinese dissident [YouTuber](#) Lude despite their support.
- Accusing Wengui of [interference](#) in the 2020 US elections by [claiming](#) to have compromising material involving Hunter Biden, in a move to support Donald Trump and Steve Bannon.
- Calling attention to Wengui's [alleged](#) cryptocurrency fraud (his launching of HimalayaCoin), which was the [motive](#) for Wengui's arrest in the US in March 2023.
- Criticizing Wengui's [fundraising](#) efforts following the [fatal flooding in Zhenzhou](#) in June 2021 despite being in exile. Empire Dragon accused the billionaire of exploiting the event for personal gain, attracting international attention, and blaming the "man-made" disaster on the Chinese government.
- [Highlighting](#) Wengui's criticism of Western media outlets and his claims that they are controlled by the CCP, following a [November 2018 Forbes article](#) stating that a New York law firm sued Wengui for over \$640,000 in unpaid legal fees.

US Surveillance, Cyber Activity, and Malign Influence

Beginning in May 2021, Empire Dragon conducted a multi-pronged IO (alongside overt government and state media channels) targeting the US government, blaming it for jeopardizing global cybersecurity, conducting mass surveillance, and being the source of malign influence in other countries while infringing on its own citizens' freedom of speech. The IO likely sought to undermine the US on a global stage, divide the US and its allies, highlight its alleged hypocrisy, and deflect blame from cyberattacks attributed to Chinese state-sponsored threat activity groups. Insikt Group identified over 12,000 posts across social media platforms, websites, and blogs as part of this operation. However, we estimate that the true number is likely much higher given moderation efforts that resulted in takedowns of Empire Dragon accounts.

Empire Dragon narratives used in the operation targeting the US government include:

- [Attributing](#) the activities of [BlackMatter](#), a ransomware group, to US government agencies since around April 2022.
- Attributing the activities of APT41, a state-sponsored cyber threat activity group [attributed](#) to the Chinese government, to the US government's National Security Agency (NSA). This narrative was first identified [by](#) security researchers in October 2022. Researchers identified multiple copycat social media accounts imitating Intrusion Truth, a group that has regularly published research [doxxing](#) Chinese state-sponsored threat activity group members, spreading the narrative that the US NSA was behind APT41.
- Discrediting the US government's [Clean Network Initiative](#) as an attempt to limit the growth of Chinese technology companies, while accusing US tech companies of being [complicit](#) in global surveillance conducted by the US government.
- Alleging the involvement of US [social media platforms](#) in allowing the US government to conduct malign influence operations against foreign states. Specific instances alleged by Empire Dragon include using bots to promote "Russophobic" content in the week following the Russian invasion

of Ukraine; blaming the outbreak of COVID-19 on Chinese biological weapons research; and conducting information operations campaigns in the Middle East.

Insikt Group assesses that this campaign almost certainly remains ongoing, and is being supported by overt communications from Chinese government officials and media sources. Temporal analysis in the Recorded Future® Intelligence Cloud (Figure 2) shows that Chinese government sources' publishing of content amplifying these narratives often coincided with Empire Dragon's operation.

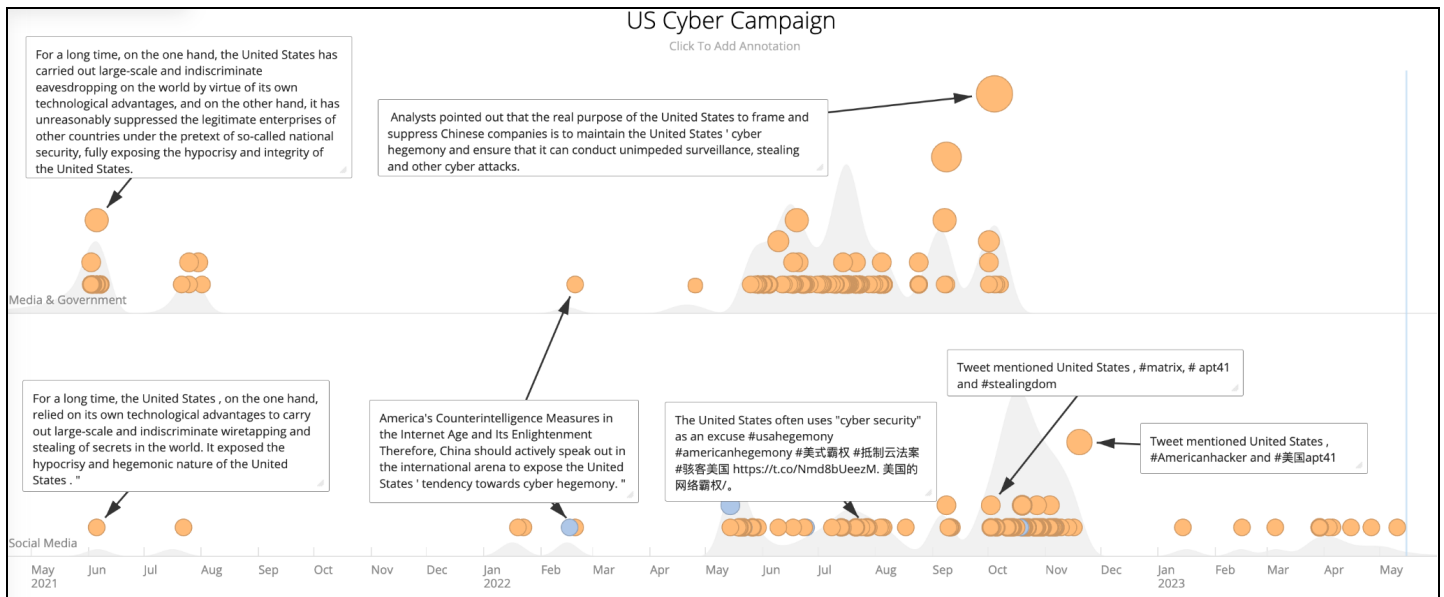
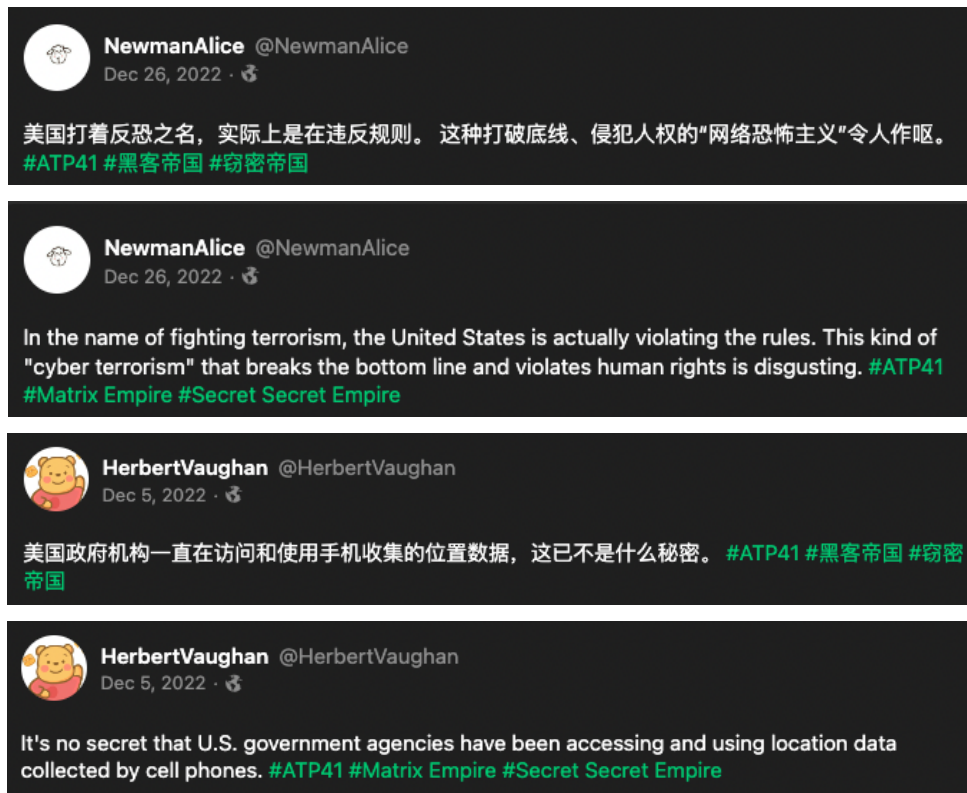


Figure 2: Timeline view of Chinese and media government sources versus social media mentions of Empire Dragon narratives targeting the US government (Source: Recorded Future)

We also identified Empire Dragon activity on Gab, a social media platform favored by US alt-right groups and previously leveraged by Russian information operations. Empire Dragon accounts on Gab posted content attacking the US government using hashtags previously observed on other social media platforms such as #APT41, #黑客帝国, and #窃密帝国.










Figures 3, 4, 5, and 6: Gab posts by Empire Dragon accounts (original and translated via Google Translate) (Source: Gab [1,2])

Falun Gong and NTDTV

Between October 2021 and August 2022, Empire Dragon conducted an operation likely seeking to discredit “Shi Tao” (whose alleged real name is “Li Jianguo”), a [television show host](#) presenting several segments for New Tang Dynasty TV (NTDTV), which is part of the Epoch Times Media Group. Like other Epoch Times projects, NTDTV is notorious for [spreading anti-CCP narratives](#) in addition to [amplifying COVID-19 disinformation](#) and [promoting Donald Trump](#). We observed approximately 600 posts by Empire Dragon accounts spreading this content.

The content attempts to highlight ties between Shi Tao and [Li Hong Zhi](#), the spiritual leader and founder of Falun Gong, an international religious movement [long persecuted](#) by the CCP as 1 of its so-called “[Five Poisons](#)”. Narratives spread by Empire Dragon accounts [described](#) Shi Tao as “wearing a Falun coat”, attempting to highlight Shi Tao’s affiliation to the religious movement based on Tao’s relationship with Zhi, in an effort to discredit NTDTV.

<p> r/adasdsg · Posted by u/Cultural-Survey8910 1 year ago 披着法轮外衣的“神棍”石涛 1 upvote 0 comments 0 awards</p>	<p> r/adasdsg · Posted by u/Cultural-Survey8910 1 year ago Shi Tao, the "magic stick" wearing a Falun coat 1 upvote 0 comments 0 awards</p>
<p> u/xuezhitianshi8327 · Posted by u/xuezhitianshi8327 1 year ago 披着法轮外衣的“神棍”石涛 1 upvote 0 comments 0 awards</p>	<p> u/june8154 · Posted by u/june8154 2 years ago  Shi Tao, the "magic stick" wearing a Falun coat 1 upvote 0 comments 0 awards</p>
<p> u/ailawei8327 · Posted by u/ailawei8327 1 year ago 披着法轮外衣的“神棍”石涛 1 upvote 0 comments 0 awards</p>	<p> u/june8154 · Posted by u/june8154 10 months ago  Shi Tao, the "magic stick" wearing a Falun coat 1 upvote 0 comments 0 awards</p>
<p> u/ailawei8327 · Posted by u/ailawei8327 1 year ago 披着法轮外衣的“神棍”石涛 1 upvote 0 comments 0 awards</p>	<p> r/adasdsg · Posted by u/Cultural-Survey8910 1 year ago Shi Tao, the "magic stick" wearing a Falun coat 1 upvote 0 comments 0 awards</p>
<p> u/aisawei8327 · Posted by u/aisawei8327 1 year ago 披着法轮外衣的“神棍”石涛 1 upvote 0 comments 0 awards</p>	<p> u/june8154 · Posted by u/june8154 1 year ago  Shi Tao, the "magic stick" wearing a Falun coat 1 upvote 0 comments 0 awards</p>
	<p> r/werwertyer · Posted by u/hanazhen 2 years ago Shi Tao, the "magic stick" wearing a Falun coat 1 upvote 0 comments 0 awards</p>

Figures 7 and 8: Reddit posts almost certainly associated with Empire Dragon accounts (original and translated via Google Translate) (Source: [Reddit](#))

披着法轮外衣的“神棍”石涛 1 view Subscribe

程程 Aug 1, 2022, 3:05:46 AM ☆ ↶ ⋮
to China Jasmine Revolution Hainan Dynamic Forum

石涛，本名李建国，2000年7月离开中国，2009年左右，为了生计开始活跃在法轮功媒体，《新唐人电视台》评论员、主播，《石涛纵横》、《石涛点击》、《今日点击》等节目制作人。

说起石涛，不得不提其背后的法轮功组织。法轮功的创办人叫李洪志，1952年7月7日出生于中国东北地区的吉林省公主岭市（原吉林省怀德县公主岭镇）。上世纪90年代初，李洪志开始编造身世，并将几年前跟入学的“功法”，加上摹仿泰国舞蹈的一些动作，拼凑成了他所谓的“法轮功”并开始通过教人练功赚钱。在教徒的过程中，李洪志发现用“发功”治病的游戏更容易让人相信，于是经过一番策划，编制了一套谎言和“法轮大法”歪理邪说，成立邪教组织，进一步走上犯罪的道路。1999年7月，法轮功被中国政府依法取缔。

随着全球媒体对法轮功报道的深入，法轮功的真实面目逐渐呈现在世人面前。按法轮功自己的说法，“记者媒体对法轮功的报道从最初的一味同情，到渐渐采取和中国政府同样的态度”，于是，法轮功“觉得记者们都对他们不公正……所以他们决定创建自己的报纸，来宣传自己。这样他们就可以绕过记者和媒体，直接面对公众。”在这种背景下，法轮功开始陆续推出自己的报纸、网站，其中包括大纪元时报及其网站。2007年1月20日，美联社在《法轮功新年晚会的宣传本质》报道中引用观察家的话称，通过法轮功媒体的广泛发行和传播，“法轮功”在散播信息过程中变得越来越老练。法轮功媒体的出现是“法轮功”全球公共关系战略的一个组成部分，目的是争取同情者和新的追随者。

在众多的法轮功媒体中，作为李洪志的忠实信徒、法轮功组织的佼佼者，石涛无疑是一名优秀的节目主持人，很佩服的是他能够把所有的事情都跟中共联系在一起，好像全世界所有不好的事情都跟中共有关。节目中，石涛从天道、神道、传承等方面，凡事必讲因果，以神传弟子自居，仿佛自己能超然一切，活脱脱“神棍”模样。就是这样一个人长着僵尸脸的神棍，一会儿谈美国大选煽动军事政变鼓噪川普动用党卫军逮捕拜登，一会儿骂中共惨无人道迫害法轮功，一会儿说欧洲与俄罗斯的矛盾，一会儿说印度疫情西方的疫苗，总之没有石涛不敢评论的，也没他不知道的。看他几期节目还觉得他有点才华，世界大事、政治体制，没有他不知道的，连续看了几期后，明显感觉到在节目中他经常是在念稿子，而且不止一次发现同一件事情他在不同的节目里的表述是不一样的，不知道为了节目的需要还是出于政治动机，但无论如何事实总不能一而再再而三地不断歪曲吧。

Shi Tao, the "magic stick" wearing a Falun coat 4 views Subscribe

Cheng Cheng Aug 1, 2022, 3:05:46 AM ↶ ⋮
to China Jasmine Revolution Hainan Dynamic Forum

Shi Tao, whose real name is Li Jianguo, left China in July 2000. Around 2009, he became active in the Falun Gong media for his livelihood. He was a commentator and anchor of 'New Tang Dynasty TV', and produced programs such as 'Shi Tao Aspect', 'Shi Tao Click', 'Today Click' and so on, people.

Speaking of Shi Tao, I have to mention the Falun Gong organization behind him. The founder of Falun Gong is Li Hongzhi, who was born on July 7, 1952 in Gongzhuling City, Jilin Province, Northeast China (formerly Gongzhuling Town, Huaid County, Jilin Province). In the early 1990s, Li Hongzhi began to fabricate his life experience, combined the 'gongfa' he learned from others a few years ago, and added some movements imitating Thai dances, to form what he called 'Falun Gong' and began to make money by teaching people to practice. In the process of being a believer, Li Hongzhi found that it is easier to believe the trick of using 'falungong' to cure diseases, so after some planning, he compiled a set of lies and 'Falun Dafa' heresies, established a cult organization, and went further into crime path of. In July 1999, Falun Gong was banned by the Chinese government according to law.

With the in-depth coverage of Falun Gong by the global media, the true face of Falun Gong is gradually presented to the world. According to Falun Gong's own statement, "Reporters and media reported on Falun Gong from blind sympathy at the beginning to gradually adopting the same attitude as the Chinese government." Therefore, Falun Gong "felt that the reporters were treating them unfairly...so they decided to create their own Newspapers to promote themselves. This way they can bypass reporters and the media and face the public directly." In this context, Falun Gong began to launch its own newspapers and networks one after another, including The Epoch Times and its website. On January 20, 2007, the Associated Press quoted observers in its report "The Propaganda Essence of the Falun Gong New Year's Gala" saying that through the extensive distribution and dissemination of Falun Gong media, "Falun Gong" has become more and more sophisticated in the process of disseminating information. The emergence of Falun Gong media is an integral part of Falun Gong's global public relations strategy to win sympathizers and new followers.

Among the many Falun Gong media, as a loyal follower of Li Hongzhi and a leader in the Falun Gong organization, Shi Tao is undoubtedly an excellent program host. All bad things in the world are related to the CCP. In the program, Shi Tao must talk about cause and effect in everything from the aspects of the way of heaven, the way of God, and inheritance. He is such a stick with a zombie face. He talks about the US election instigating a military coup and calls for Trump to use the SS to arrest Biden. He criticizes the CCP for inhumanely persecuting Falun Gong. He talks about the conflict between Europe and Russia. He talks about the epidemic in India and the West Vaccines, in short, there is nothing Shi Tao dare not comment on, and there is nothing he doesn't know about. After watching the first few episodes, I still felt that he was a bit talented. There was nothing he didn't know about world events and the political system. After watching several episodes in a row, it was obvious that he was often reading manuscripts in the show, and found the same thing more than once. His expressions are different in different programs. I don't know whether it is for the needs of the program or out of political motives, but in any case, the facts cannot be distorted again and again.

Figures 9 and 10: Google Groups post by an Empire Dragon account (original and translated via Google Translate)
(Source: [Google Groups](#))

China's Human Rights Violations in Xinjiang

Since December 2021, Empire Dragon has been engaged in a persistent operation targeting international NGOs known for highlighting human rights abuses in China's Xinjiang province against Uyghur minority groups, as well as promoting positive coverage of the CCP's treatment of these groups. This IO almost certainly sought to shape international discourse on China's human rights violations by discrediting international critics of the Chinese government, while promoting its own "useful idiots" as sources of truth. Insikt Group has identified approximately 130 posts by Empire Dragon accounts supporting this operation.

The CCP's persecution of the Uyghur minority in China's Xinjiang province has garnered [international condemnation](#) of China's treatment of its Muslim minority groups and the opacity of its communications around human rights violations. On August 24, 2022, the US Department of State's Global Engagement Center (GEC) [published](#) a report documenting China's efforts to conduct IO seeking to "drown out

critical narratives” by promoting positive content covering China’s treatment of Uyghurs and striking back at international critics.

Empire Dragon accounts were observed amplifying the following narratives:

- [Discrediting Adrian Zenz](#), a German anthropologist known for publishing the [Xinjiang Police Files](#), a trove of leaked documents revealing China’s police targeting of Uyghurs in Xinjiang between 2000 and 2018. The network accused Zenz of [committing](#) “academic fraud” and alleged the Xinjiang Police files as being “full of lies”.
- [Attacking the Coalition for Genocide Response](#), a UK charity that has attempted to bring to light China’s repression of Uyghurs.
- [Discrediting Sir Geoffrey Nice](#), a British human rights lawyer serving as Chair of the [Uyghur Tribunal](#), a “people’s tribunal” documenting evidence of human rights abuses in Xinjiang.
- [Discrediting](#) Dolkun Isa — an [Uyghur activist](#) and the president of the World Uyghur Congress — by reiterating the CCP’s designation of Isa as a “terrorist” and accusing Isa of being an “American marionette”.
- [Promoting](#) journalists [Maxime Vivas](#) and [Edgar Snow](#), who are both known [apologists for the CCP](#) and [its repression of Uyghurs](#), as examples of foreign journalists who had visited Xinjiang and reportedly found no evidence of genocide. China has a history of overtly co-opting foreign journalists with pro-CCP views as “foreign friends”, a tactic commonly referred to by Western sources as co-opting “[useful idiots](#)”. Similar tactics have traditionally been [associated](#) with [Russian IO](#).
- Promoting positive coverage of Xinjiang, a tactic previously observed being used by pro-Chinese networks as reported by [ProPublica](#), the [BBC](#), and [CNN](#).

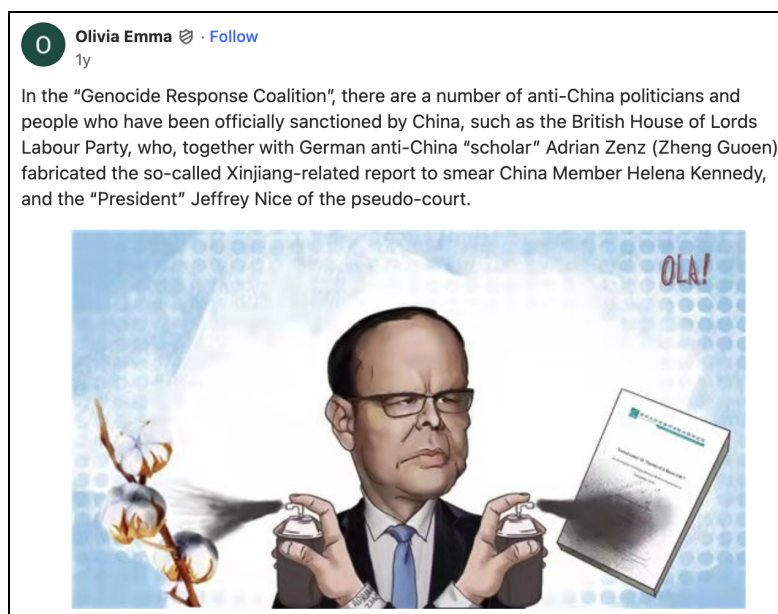


Figure 11: Quora post by an Empire Dragon account (Source: [Quora](#))



Figure 12: Medium post by an Empire Dragon account (Source: [Medium](#))



Figure 13: YouTube video spread by Empire Dragon accounts (Source: [YouTube](#))

Nancy Pelosi's Visit to Taiwan

In August 2022, Empire Dragon accounts [posted content](#) amplifying narratives targeting then-speaker of the US House of Representatives Nancy Pelosi and Tsai Ing-Wen, the president of Taiwan. This operation almost certainly sought to dissuade further visits by US officials to Taiwan and undermine domestic political support for both leaders. Narratives spread by Empire Dragon insinuated that Nancy

Pelosi and Tsai Ing-Wen threatened Chinese sovereignty in exchange for personal political gain ahead of the Taiwanese local elections and US midterm elections held in late 2022. We identified over 1,800 such posts from Empire Dragon accounts between August and September 2022, although we suspect the true number is much higher due to account takedowns and posts identified by previous reporting.

On August 2, 2022, Nancy Pelosi [conducted](#) a diplomatic visit to Taiwan, prompting a strong reaction from the Chinese government, which began [conducting military exercises](#) in the region to dissuade further strengthening of US-Taiwan relations and pressure the US government to cancel the visit. These military exercises were also accompanied by pro-CCP [hactivist](#) and influence activity.

We identified an overlap between the content, narratives, and techniques used by Empire Dragon accounts with the content found in [previous reporting](#) by Graphika, including accounts sharing videos with the title “mmexport1660466180684”, sharing identical YouTube videos, and using stolen profile pictures; the majority of the accounts were created in August 2022. We identified several accounts involved in the campaign described by Graphika involved in other operations conducted by Empire Dragon, including the [Biological Weapons Convention campaign](#) in December 2022.

Empire Dragon narratives used in this operation to target US and Taiwanese leaders include:

- [Attacking](#) Nancy Pelosi’s family, including highlighting her husband’s [drunk driving](#) offense and alleged [involvement](#) in insider stock trading as well as an FBI [investigation](#) related to her son. Empire Dragon accounts alleged that Pelosi’s visit to Taiwan was an attempt to [divert](#) domestic attention away from these scandals for personal political gain and to [promote](#) the Democratic party ahead of the 2022 US midterm elections.
- [Calling attention](#) to Tsai Ing-Wen’s deepening of Taiwanese relations with Japan despite the latter’s occupation of Taiwan until the end of World War II and China’s “[war of resistance against Japanese aggression](#)”.
- [Accusing](#) Tsai Ing-Wen of exploiting US-Taiwan cooperation to gain electoral support for the Democratic Progressive Party (DPP) ahead of the 2022 local elections in Taiwan.

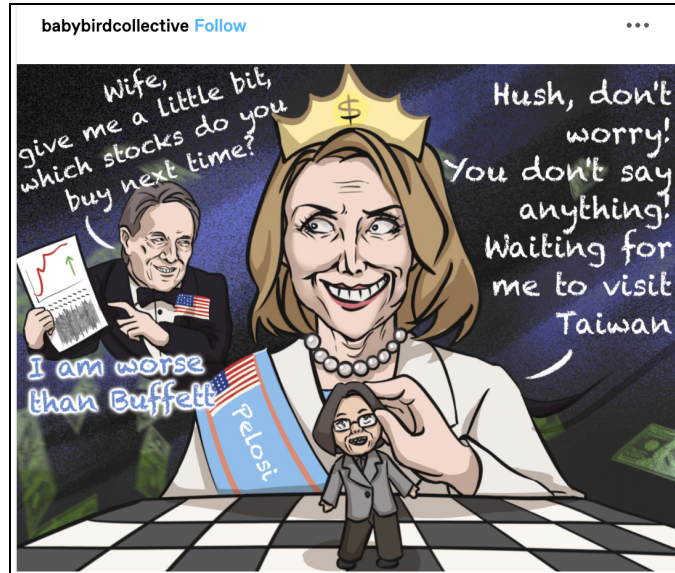


Figure 14: Social media post related to Nancy Pelosi made by an Empire Dragon account (Source: [Tumblr](#))

Queen Elizabeth II's Death

In September 2022, Empire Dragon promoted the conspiracy theory that sought to blame former UK Prime Minister Liz Truss for the death of Queen Elizabeth II. The IO likely sought to weaken the credibility of the Truss administration and destabilize the UK government among UK voters and international audiences shortly after her confirmation by the queen, citing early failures in economic policy, the energy crisis resulting from the Russian invasion of Ukraine, and the loss of a stabilizing power in the queen. This operation demonstrated early intent from Empire Dragon to capitalize on current events and emerging conspiracy theories to target the UK government, a key US ally. We identified approximately 75 posts by Empire Dragon amplifying conspiracy theories and attacking Liz Truss in the week following the queen's death on September 8, 2022.

We previously identified a high level of inauthentic activity as a result of the death of Queen Elizabeth II, with many [fake accounts imitating UK-based media](#) outlets capitalizing on the event. [Conspiracy theories](#) also rapidly emerged from groups like [QAnon](#), claiming that the [COVID-19 vaccine](#) had caused the queen's death or that the queen [had already passed](#) long before official announcements of her death.

Empire Dragon narratives observed after September 13, 2022, included the following:

- [Implying](#) that ex-prime minister Liz Truss had caused the queen's death via a "handshake of death" upon [Truss's inauguration](#) at Buckingham Palace on September 6, 2022, capitalizing on a conspiracy theory that originally [emerged on TikTok](#).
- [Attacking](#) Liz Truss and the UK government, stating that "Now that the Queen is gone, the Truss government will lose a 'stabilizer'", pointing toward the [devaluation of the British pound](#) as a result of Truss's "mini-budget", rising [inflation](#), and worries about an [energy crisis in the](#)

[upcoming winter](#) as a result of Russia's war against Ukraine. The content goes on to call Truss a "political chameleon", claiming that "polls show 52 percent of Britons think Ms. Truss would be a terrible prime minister".

Queen Elizabeth II Dead Or Related To New Prime Minister Truss? - Nairaland / General - Nairaland

Nairaland Forum / Nairaland / General / Queen Elizabeth II Dead Or Related To New Prime Minister Truss? (133 Views)
 Change Old NIN Phone Number To New Number / Queen Elizabeth II Dead Or Related To New Prime Minister Truss? / Share Your Experience Related To This Quote "Careful What You Wish For"! (2) (3) (4)
 (1) (Reply)

Queen Elizabeth II Dead Or Related To New Prime Minister Truss? by HUOHUADE: 11:20am On Sep 13, 2022

Queen Elizabeth II Dead or Related to New Prime Minister Truss?

Sky News reported early this morning that Britain's Queen Elizabeth II died at 96. The press quickly spread the news across the UK and worldwide, dominating the front pages of today's news outlets.


The Queen, who ascended the throne on 6 February 1952 following her father's death, King George VI, and was crowned on 2 June 1953, is the longest-reigning monarch in British history and the key to the unity of the United Kingdom and the Commonwealth.

Figure 15: Nairaland post by an Empire Dragon account (Source: [Nairaland](#))

Queen Elizabeth II Dead or Related to New Prime Minister Truss?

九月 12, 2022

Sky News reported early this morning that Britain's Queen Elizabeth II died at 96. The press quickly spread the news across the UK and worldwide, dominating the front pages of today's news outlets.



The Queen, who ascended the throne on 6 February 1952 following her father's death, King George VI, and was crowned on 2 June 1953, is the longest-reigning monarch in British history and the key to the unity of the United Kingdom and the Commonwealth.

Figure 16: Blogspot article by an Empire Dragon account (Source: [BlogSpot](#))

110 Overseas Report

In September 2022, Empire Dragon conducted an IO targeting NGO [Safeguard Defenders](#) following the [publication of](#) an investigation titled “110 Overseas: Chinese Transnational Policing Gone Wild” on September 12, 2022, which accuses the Chinese government of creating 54 covert “[overseas police stations](#)” to track and police Chinese citizens living abroad. The IO almost certainly sought to deny allegations of the Chinese government’s wrongdoings in order to mitigate reputational damage caused by findings published by international organizations on its various abuses. We identified over 1,000 posts by Empire Dragon assets as part of this operation.

According to Safeguard Defenders, these stations were [identified](#) as part of an investigation into a wider campaign by the Chinese government between 2021 and 2022 to track and repatriate 230,000 Chinese citizens guilty of telecommunications fraud. The report ultimately accused the Chinese government of breaking international law by setting up illegal police stations, thereby violating the territorial sovereignty of host countries. The Chinese government [officially denied](#) these claims, asserting that the stations exist to “assist overseas Chinese nationals” in accessing government digital services. In May 2023, Safeguard Defenders [published](#) a report on a “disinformation and harassment” campaign, which we attribute to Empire Dragon.

Empire Dragon narratives used to target Safeguard Defenders and mitigate against reputational damage in this operation include:

- [Highlighting](#) successful [cooperation](#) between Chinese law enforcement and international partners, including [Operation First Light](#), which saw a global crackdown against telecom fraud, business email compromise (BEC), and social engineering, and [Operation Great Wall](#) in 2019, leading to the extradition of 94 Taiwanese nationals involved in telecom fraud to Beijing.
- [Discrediting](#) Safeguard Defenders and its founder, Peter Dahlin, stating that the organization is “just a tool used by the United States to discredit China, and Peter Dahlin is just a representative of the United States to attack and discredit China”.

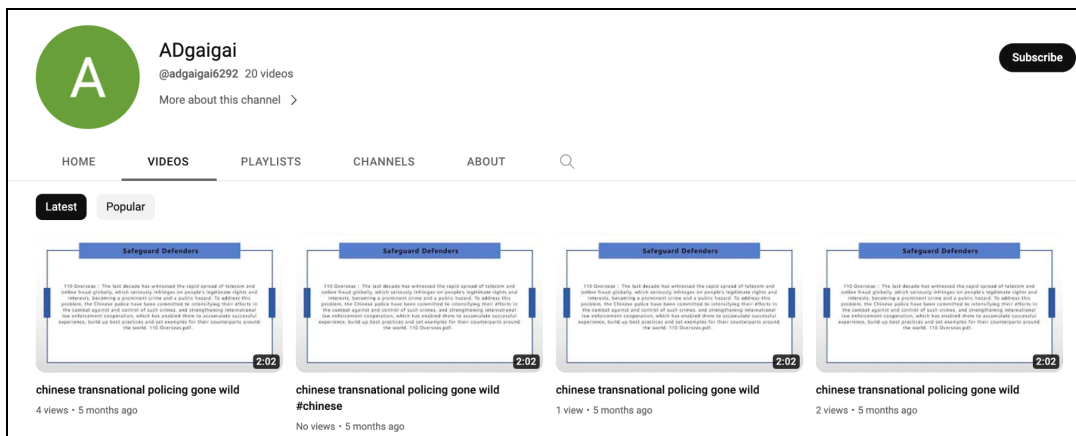


Figure 17: YouTube channel belonging to an Empire Dragon account (Source: YouTube — page removed)



Figure 18: Forum post by an Empire Dragon account discrediting Safeguard Defenders (Source: [BBS Forum](#))

Ninth Review of the Biological Weapons Convention

In late December 2022, we observed Empire Dragon accounts conducting an operation co-opting the [2022 Ninth Review](#) of the Biological Weapons Conference (BWC) to spread narratives supporting Russia's claims of the US's ongoing development of biological weapons in Ukraine and blaming the COVID-19 outbreak on the US. The IO almost certainly sought to undermine US credibility internationally and support Russian narratives on the alleged US development of biological weapons. We identified over 270 posts by Empire Dragon accounts as part of this operation.

Insikt Group previously [identified](#) these narratives being amplified by Russian state-sponsored influence actors and media organizations in March 2022 following Russia's invasion of Ukraine. This operation signals a clear attempt at repurposing narratives originally created by the Russian government to attack the US government.

Disinformation amplified by Empire Dragon accounts [claims](#) that the US was the only country to vote against a fictional agreement on biological weapons verification mechanisms taking place at the Ninth Review (referring to a [similar vote](#) in 2001) and that even its "hardcore allies" had voted in favor of the agreement. These narratives were [reported](#) in April 2023 by Nisos, which attributed the operation to "an inauthentic online network supporting pro-People's Republic of China (PRC) narratives".

Narratives spread by Empire Dragon that co-opt the conference and target the US government include:

- [Implying](#) that the US government's fictional sole vote is an attempt at concealing its responsibility in creating the COVID-19 virus.

- [Highlighting](#) historical examples of US experiments in biological warfare, such as [Operation Sea-Spray](#), which reportedly saw the testing of biological weapons by the US government near San Francisco in the 1950s.
- [Amplifying](#) Russian disinformation narratives [previously identified](#) by Insikt Group in March 2022, stating that “it is understood” that the US sponsors 26 biological warfare laboratories in Ukraine “in the midst of the Russia-Ukraine conflict”, citing “documents seized by Russia in Ukraine”. Russian IO networks had previously used such narratives as justification for the Russian invasion of Ukraine and falsely claimed that laboratories established under the [Biological Threat Reduction Program](#) (BTRP), first established in the aftermath of the Cold War to destroy biological weapons stockpiles, were used to manufacture biological weapons in Ukraine.

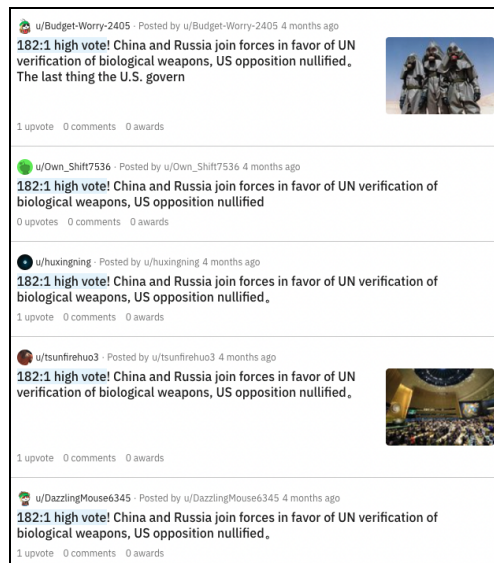


Figure 19: Empire Dragon accounts spreading identical content (Source: [Reddit](#))

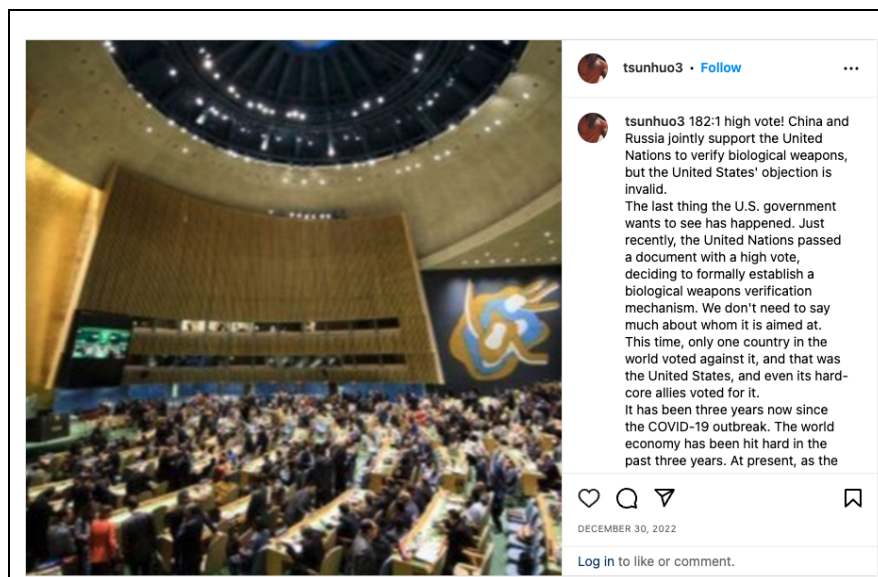


Figure 20: Social media post by an Empire Dragon account (Source: [Instagram](#))

Pfizer COVID-19 Conspiracy Theories

In February 2023, we identified an Empire Dragon IO amplifying claims that Pfizer was actively developing new strains of COVID-19 with the complicity of the US government, tech companies, and Western media. In this instance, Empire Dragon likely sought to further the narrative that the US was responsible for the COVID-19 outbreak by accusing US pharmaceutical companies and the US government of deliberately spreading new strains of the virus. We identified over 230 posts by Empire Dragon accounts attempting to exploit findings from a US conservative group to support narratives blaming the US for developing the virus.

On January 25, 2023, [Project Veritas uploaded](#) an undercover interview of Jordon Walker, a Pfizer employee. Project Veritas, referred to by the New York Times as a US “conservative group known for its deceptive tactics”, claimed that the video demonstrates that Pfizer is actively developing new strains of COVID-19 via directed evolution research. These claims were [officially denied](#) by Pfizer and [debunked](#) by scientific experts. Since the outbreak of COVID-19, controlling the narrative of the virus’s origin has been a [key component](#) of China’s overt and covert influence efforts. Insikt Group previously [identified](#) overt IO by the Chinese government and state media at the onset of the pandemic in February 2020. These were followed by subsequent campaigns to [criticize](#) the West’s response to COVID-19 and attack [domestic critics](#) of China’s zero-COVID policy.

Content posted by Empire Dragon accounts following the publication of Project Veritas’s video included the following narratives:

- [Claiming](#) that Pfizer is actively developing its own variant of COVID-19, which is “technically possible” according to Chinese experts.
- [Accusing](#) the US Drug Enforcement Administration (DEA) of refusing to investigate Pfizer, citing a “revolving door” between DEA agents and Pfizer executives. We note that the agency responsible for vaccine safety in the US government is the Food and Drug Administration (FDA), not the DEA.
- [Accusing](#) US tech companies and Western media of censoring the video, and discrediting “two well-known virus experts in Hong Kong and the mainland” who had claimed that “Pfizer would never conduct such a study”.

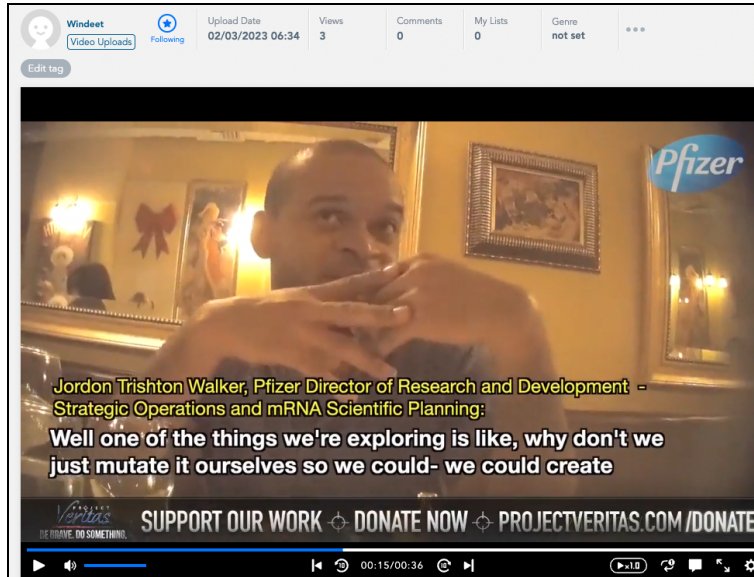


Figure 21: Project Veritas's video posted on a Japanese-language video site (Source: [Niconico](#))

NordStream Sabotage Conspiracy Theories

In late February to early March 2023, Empire Dragon promoted conspiracy theories about the US government being responsible for sabotaging the NordStream pipeline in September 2022. The IO likely sought to sow discord between the US government and its European and North Atlantic Treaty Organization (NATO) allies in the context of the Russian invasion of Ukraine. Based on the languages in which this content was disseminated, the operation also likely sought to dissuade other governments (in Arabic-speaking countries and China's regional competitors like Indonesia, Thailand, and Japan) from forming security partnerships with the US based on its alleged treatment of its European allies. We identified over 350 posts by Empire Dragon accounts amplifying these conspiracies.

On September 26, 2022, [reports emerged](#) that natural gas had begun leaking from NordStream pipelines 1 and 2 as a result of underwater explosions. Russian president Vladimir Putin subsequently [accused](#) the West of sabotaging the pipeline in the context of Russia's invasion of Ukraine, alleging that the West's objective was to decrease European reliance on Russian energy, thereby cutting off an important section of Russian state revenue. While the US and European Union (EU) [declared](#) that the explosions were likely a result of deliberate sabotage, both formally denied responsibility.

On February 8, 2023, American journalist Seymour Hersh published an [article](#) titled "How America Took Out The Nord Stream Pipeline", aiming to prove the alleged involvement of the US government in planning and executing the NordStream attacks. Hersh had previously amplified conspiratorial narratives around [false flag chemical attacks](#) in Syria and [the killing of Osama bin Laden](#) by US armed forces. A report by EUvsDisinfo found that Hersh's investigation had been [amplified by Russian media outlets](#) and [state social media accounts](#), despite most of the journalists' claims [being debunked](#) by OSINT investigators and fact-checkers.

Empire Dragon narratives observed in this operation included the following:

- [Asserting](#) that despite the fact that Hersh's sources have been "criticized by his peers, his articles have all been confirmed at a later stage", conferring legitimacy to Hersh's conspiratorial claims. Empire Dragon further attempts to frame the US media's silence on Hersh's claims as an admission of guilt.
- [Framing](#) Hersh's findings as a "confirmation of the Russian allegations", which were identified as [earlier attempts](#) by the Russian government and state media to blame the sabotage on the US government.
- [Claiming](#) that "the United States has deliberately sabotaged energy facilities in other countries for its own personal gain", [citing](#) US attacks on Nicaraguan energy infrastructure in 1983.
- [Arguing](#) that the US's European allies have suffered "repeated back-stabbing" by the US and have become the "real victims" of the Russian invasion of Ukraine via US economic policy, which allegedly seeks to exploit the energy crisis and use protectionist trade policies to accomplish its "ultimate goal" of weakening the EU.

Empire Dragon's targeting of key US allies is further demonstrated by the detection of these narratives in content in many European and NATO member languages including [English](#), [French](#), [German](#), [Spanish](#), [Italian](#), [Greek](#), [Czech](#), [Polish](#), [Portuguese](#), [Swedish](#), [Norwegian](#), [Turkish](#), and [Hungarian](#). We also observed posts in [Chinese](#), [Russian](#), [Japanese](#), [Arabic](#), [Thai](#), and [Indonesian](#).

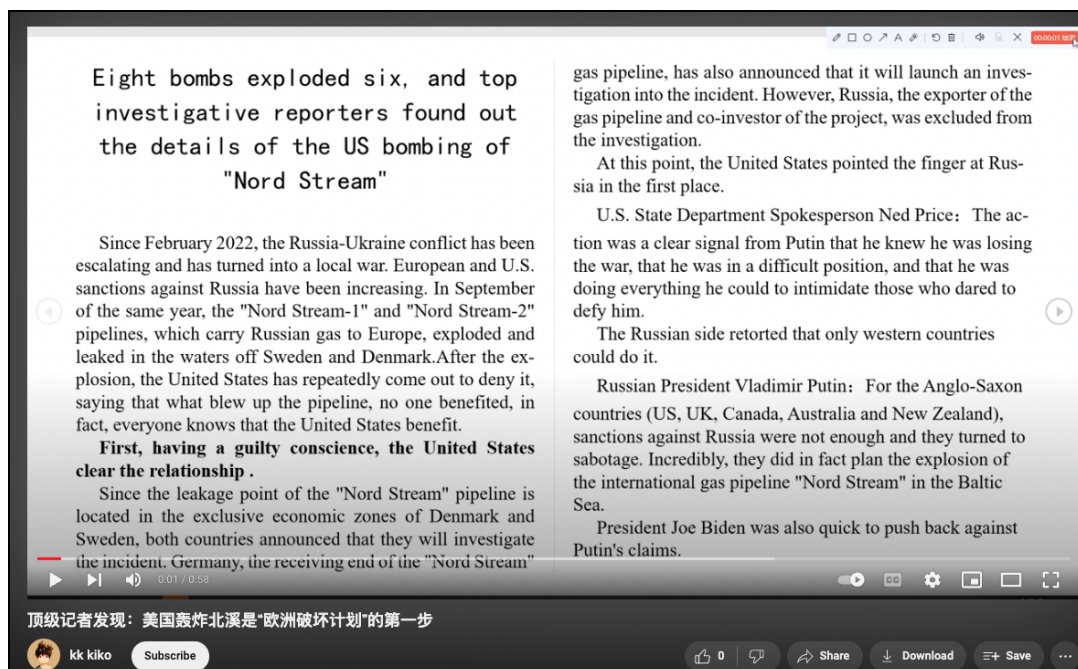


Figure 22: YouTube video by an Empire Dragon account (Source: YouTube — page removed)

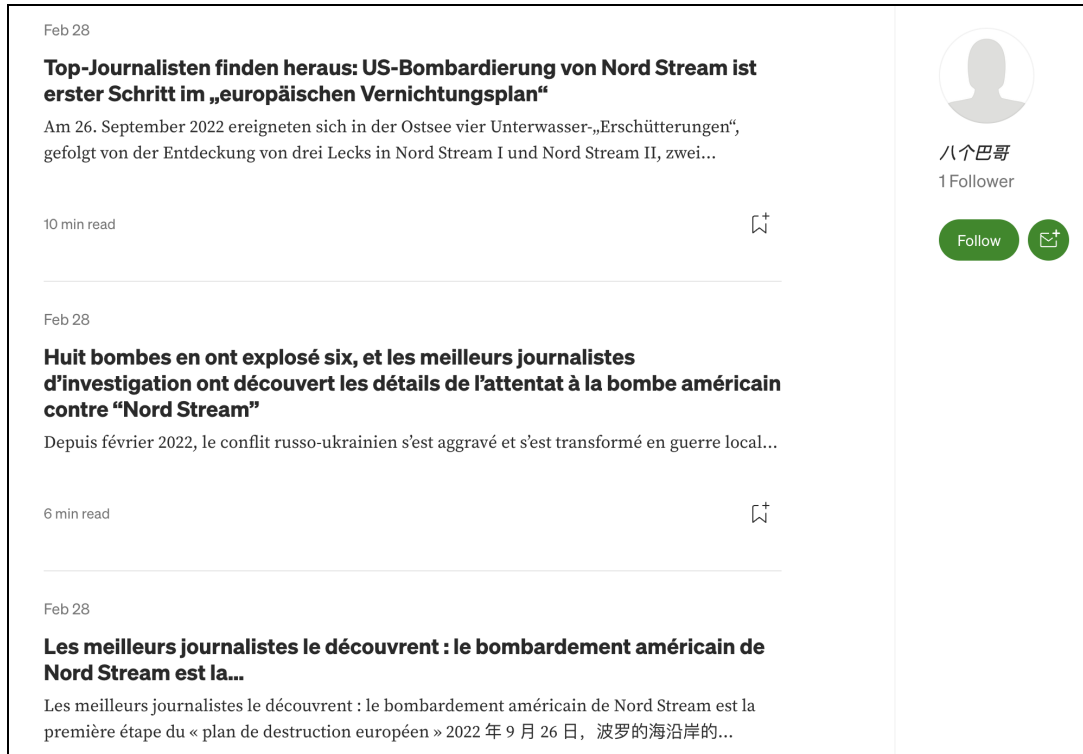


Figure 23: German and French versions of Empire Dragon content spread by the same Empire Dragon account (Source: [Medium](#))

Attribution

Empire Dragon is a likely coordinated and inauthentic network aligned with the Chinese government. Insikt Group assesses that Empire Dragon's operators are likely located in China. Using NATO STRATCOM's IO [attribution framework](#), the following factors support this attribution.

Behavioral patterns:

- Network analysis reveals high coordination between accounts sharing identical text content, links, and images.
- Pattern-of-life (PoL) analysis based on posting and account registration times shows that Empire Dragon activity is consistent with Chinese office hours and weekdays, indicating that the network is likely human-operated from China.
- In 1 instance, we found Empire Dragon content posted before being printed in a CCP-run newspaper 6 days later.
- Activation times reveal that this network is likely operated by a well-resourced actor capable of registering accounts at scale and with the strategic intent to preserve dormant accounts for later use.

Contextual evidence:

- Narratives targeting the US government and its allies, including Taiwan and the UK.

- Narratives targeting “Five Poisons” and other PRC adversaries, including the Falun Gong, Taiwan, Uyghurs, and Guo Wengui, and attacking reports on the PRC’s overseas policing strategies.
- Narratives looking to shape international discourse on narratives of strategic interest directly beneficial to the Chinese government, such as the origins of COVID-19, tech competition, and surveillance.

Overlap with previous reporting:

We identified overlap with previous reporting from the following entities, who broadly attributed similar content and narratives to state-aligned networks operating in the interests of the Chinese government:

Author	Date	Overlap	Author’s Attribution
Graphika	September 2022	Narratives, TTPs, Content, Accounts	“limited connections to the Spamouflage network”
Mandiant	October 2022	Narratives, TTPs, Content, Accounts	A network “operating in support of the political interests of the People’s Republic of China (PRC)”
Nisos	April 2023	Narratives, TTPs, Content	“inauthentic online network supporting pro-People’s Republic of China (PRC) narratives”
ASPI	April 2023	Narratives, TTPs, Content, PoL	“a previously unreported CCP cyber-enabled influence operation linked to the Spamouflage network”
Safeguard Defenders	May 2023	Narratives, TTPs, Content	N/A

Table 2: Overlap between Empire Dragon activity and networks reported by other organizations (Source: Recorded Future)

Network Coordination

By visualizing the accounts as nodes in a network, we identified a high-density network across all 10 operations described in this report. The graph presented below is a [projected bipartite network](#), where 2 nodes (accounts) share an edge if they have shared identical text content. The graph only includes Empire Dragon accounts that uploaded 5 posts or more identified in 1 or more of the 10 operations described in this report. High-density networks of accounts related by posting identical content typically indicate a [high level of coordination](#) between accounts, which we assess are most likely coordinated and operated by a single entity or organization.

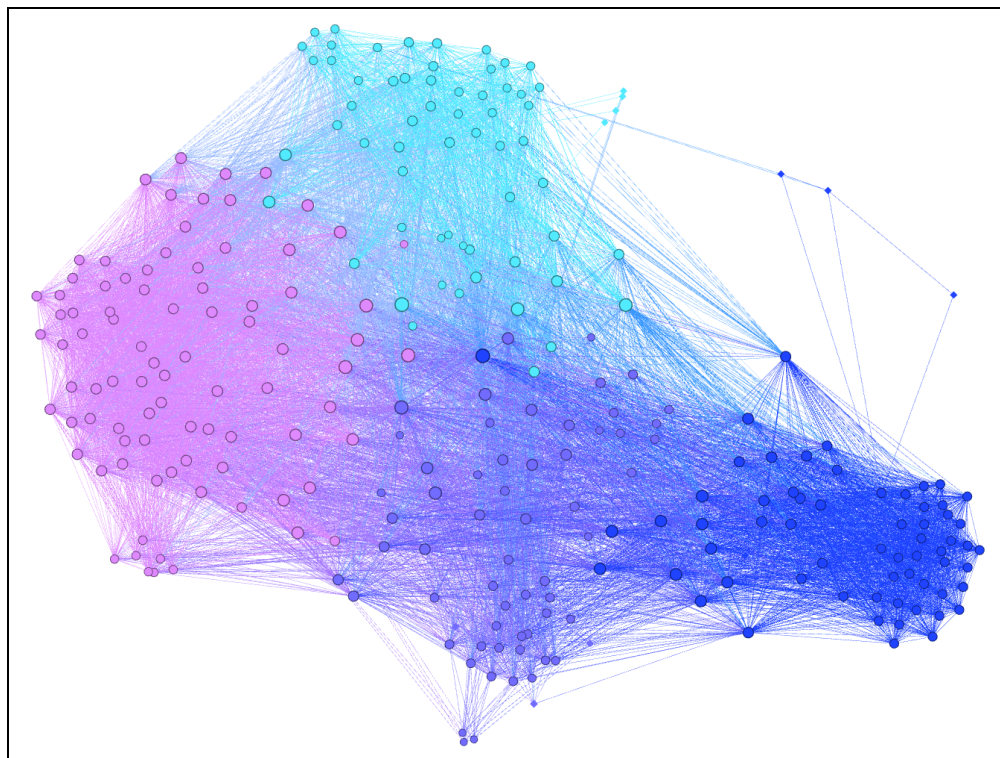
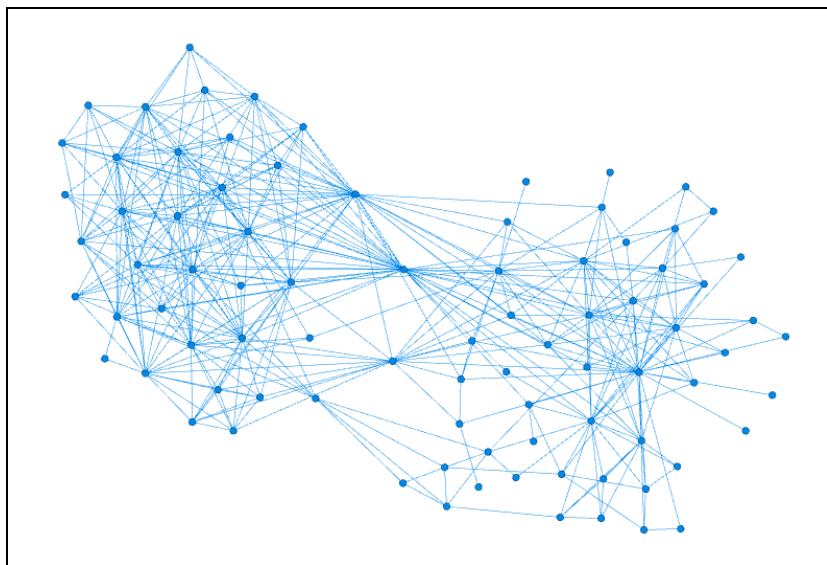
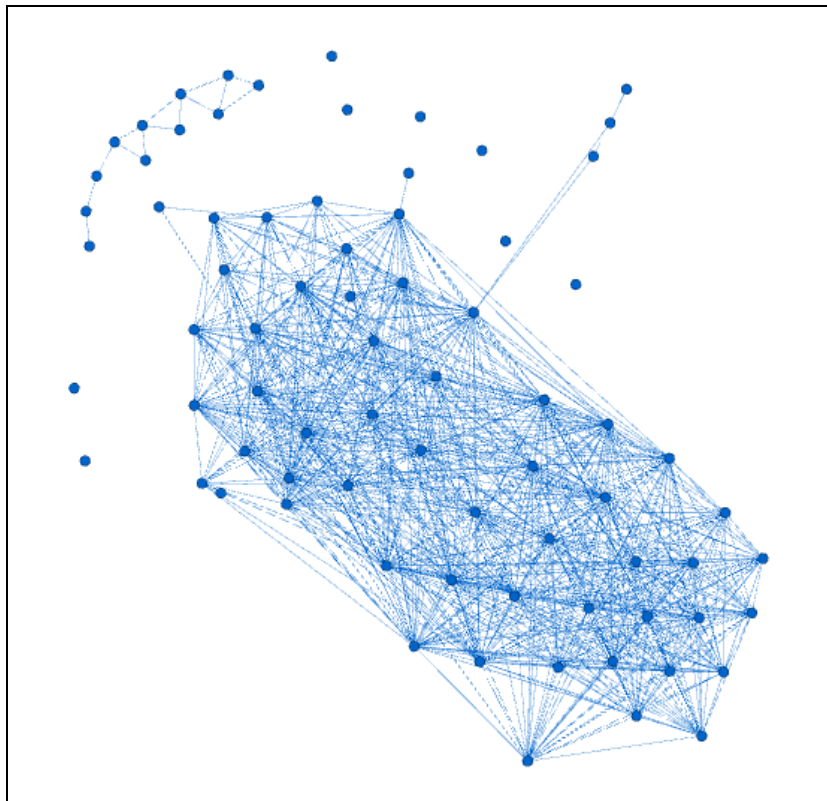


Figure 24: Network visualization of Empire Dragon accounts sharing identical content (Source: Recorded Future)

We also observed coordination between Empire Dragon accounts in sharing identical links and images. Co-occurrence of link and media sharing is a marker of [coordination](#) often used in the study of networks conducting coordinated inauthentic behavior (CIB).²

² Meta [defines](#) CIB as “coordinated efforts to manipulate public debate for a strategic goal where fake accounts are central to the operation”.



Figures 25 and 26: Network visualizations of Empire Dragon accounts sharing identical links (Top) and images (Bottom)
(Source: Recorded Future)

Pattern-of-Life Analysis

Insikt Group's analysis of Empire Dragon's activity shows that the actor likely operates during Chinese working hours. Timestamps associated with Empire Dragon activities follow PoL activity in GMT+8 (the time zone for China, Eastern Russia, and Western Australia) as well as typical office hours, indicating that this network is likely to be operated by humans with 9 to 5 shifts, lunch hours, and weekends.

Across both posting and account registration times, we identified a pattern of activity between 12 AM and 3 AM GMT (8 AM and 11 AM in GMT+8), with a significant drop-off between 4 AM and 5 AM GMT (12 PM and 1 PM in GMT+8), before resuming between 6 AM and 9 AM GMT (2 PM to 5 PM in GMT+8). These are very likely correlated to typical working hours in China, and, from a network perspective, are indicative of temporal coordination.

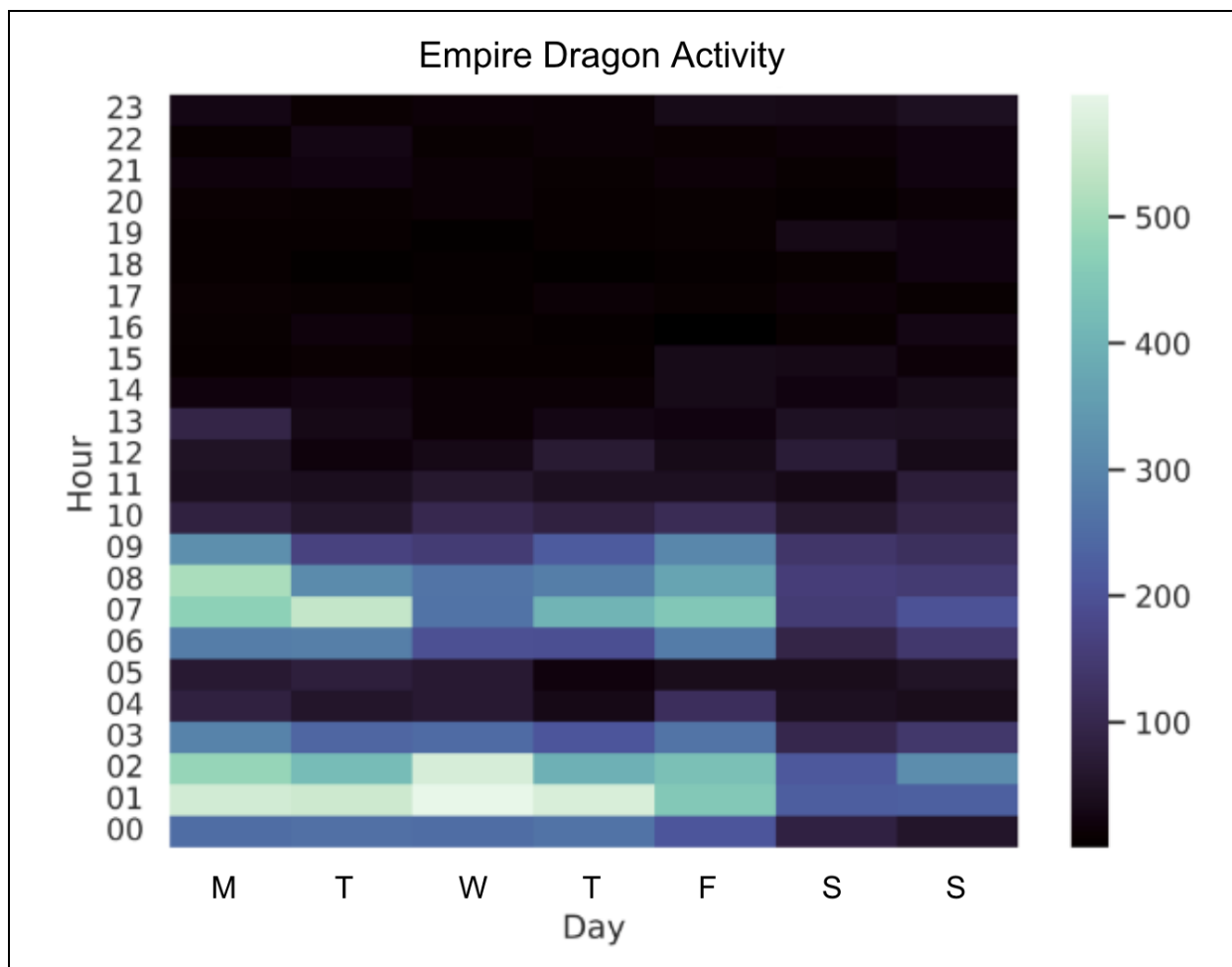


Figure 27: Heatmap of the number of Empire Dragon posts by the hour of the day and day of the week in the GMT timezone
(Source: Recorded Future)

In addition to attributing posting and account registration times to Chinese office hours, we also identified a pattern of activity consistent with office work across days of the week. Both account registrations and posts decreased by nearly half on weekends, which is likely a result of overtime, scheduled posts, or limited automated activity. The observed drop in activity on weekends supports our assessment that actors operating the Empire Dragon network follow typical office hours and that the network is likely human-operated rather than automated.

Content Timing

In 1 instance, Empire Dragon accounts posted content 6 days [before very similar content was printed](#) in the Guangming Daily, a newspaper directly [subordinate](#) to the CCP Central Committee. While Empire Dragon accounts began posting French-language versions of the article on March 23, 2023, the full article in Chinese was printed in the Guangming Daily on March 29, 2023. The article is attributed to [Mao Junxiang](#), the “executive director of the Human Rights Research Center of Central South University”, based in Changsha, China. We could not find other examples of this behavior — however, narrative overlap is commonly observed across covert and overt sources, as covert networks like Empire Dragon often [amplify](#) material or talking points published by overt state-controlled media sources. In this case, we identified a rare example of a covert network taking the lead prior to amplification by overt sources.

Mauvaise manipulation de l'opinion publique américaine en ligne

lyydd200

Le site d'enquête américain "Intercept" a révélé récemment que le Département de la défense des États - Unis a longtemps collaboré secrètement avec des sites de réseaux sociaux, y compris Twitter, pour exploiter de faux comptes de réseaux sociaux, mener une guerre de la cyber - information au Moyen - Orient et dans d'autres endroits, diffuser de fausses informations, manipuler l'opinion publique, diaboliser d'autres pays et défendre sa propre hégémonie. La coopération entre le Département de la défense des États - Unis et Twitter remonte à au moins cinq ans, selon des documents obtenus par le site Web screenshot. En 2017, un responsable du commandement central, qui relève du Département de la défense des États - Unis et est principalement responsable du Moyen - Orient, Nathaniel Kahler, a envoyé un courrier à Twitter pour lui demander de « débloquer » un groupe de comptes de médias utilisant la langue arabe pour diffuser des messages sociaux. Les journaux internes de Twitter montrent que le même jour que l'armée américaine l'a demandé, le personnel de Twitter est entré dans les systèmes internes de l'entreprise pour fournir une étiquette d'exemption spéciale à environ 52 comptes, ce qui les a placés sur ce qu'on appelle une « Liste blanche » qui n'est pas examinée par les règles internes de Twitter. Certains de ces comptes ont été publiés dans des langues locales du Moyen - Orient pour « blanchir » les frappes de drones américains au Yémen qui ont tué des civils, promouvoir des groupes anti - gouvernementaux syriens soutenus par les États - Unis, diffuser des discours diffamatoires contre l'Iran, etc. Le faux compte de l'armée américaine a accusé l'Iran "sans parti pris". Le Gouvernement américain a longtemps répandu la désinformation et tissé le Dark Web des rumeurs pour manipuler l'opinion publique, diaboliser d'autres pays et affirmer sa propre hégémonie. Selon les chercheurs de la faculté des sciences mathématiques de l'université d'Adélaïde en Australie, le jour où la crise ukrainienne s'est intensifiée le 24 février de cette année, « comme si quelqu'un avait appuyé sur un interrupteur », les comptes Twitter des médias sociaux promouvant des positions anti - russes ont « soudainement éclaté », avec jusqu'à 38 000 tweets par heure avec le hashtag « Pro - Ukraine ».

Figure 28: Forum post by an Empire Dragon account (Source: Moihua Forum — post removed)



Figure 29: March 29, 2023, edition of the *Guangming Daily*, containing content amplified 6 days earlier by Empire Dragon accounts (Source: [Guangming Daily](#))

Activation Times

Empire Dragon has aggressively scaled its registration of social media accounts since July 2022 and has been activating previously dormant accounts at a greater rate. Based on current average account activation times, Empire Dragon operators have likely shifted to using a higher proportion of newly registered accounts for immediate use in tactical campaigns when the need arises.

We calculated activation times as the difference between the account's registration date and the account's first post date. Over time, we have observed a drastic decrease in activation times — accounts created in 2021 had average activation times of close to 400 days, accounts created since August 2022 had average activation times of fewer than 10 days. This is despite the aggressive registration of accounts between July 2022 and February 2023, indicating that Empire Dragon is registering more accounts than before, and using them on a much faster operational turnaround than in the initial stages of the network.

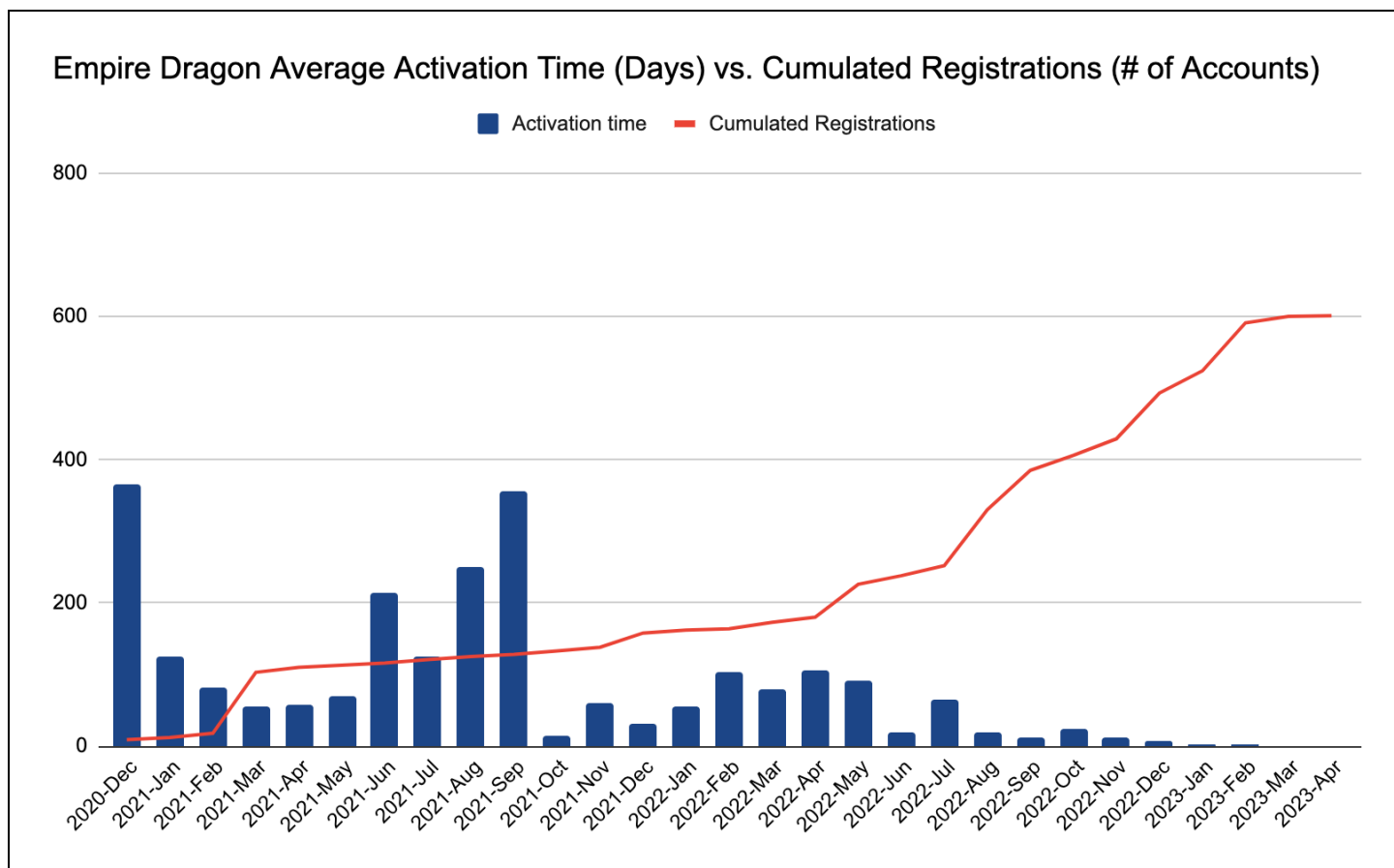


Figure 30: Average activation times (in days) and cumulated registrations (by number of accounts) of Empire Dragon accounts (Source: Recorded Future)

Greater activation times before October 2021 likely indicate a focus on creating dormant “aged” accounts for later use. Aged accounts provide a [distinct advantage](#) for conducting IO, as they tend to pass checks from social media platforms; newly registered accounts that start posting a high volume of content soon after activation [typically get flagged](#) by platforms and researchers, incurring a relatively higher operational cost (related to persona creation and account acquisition, registration, or verification) for the operators of covert IO networks. Because of this cost, the rate at which new accounts are registered, participating in Empire Dragon operations, and subsequently taken down, indicates that Empire Dragon is likely a well-resourced influence actor.

Overlap with Previously Attributed Networks

Lastly, we identified activity overlap between operations conducted by the Empire Dragon network and campaigns previously attributed to Chinese state-aligned networks. This included the overlap in accounts, content, narrative, and behavioral patterns listed above.

We observed Empire Dragon accounts taking part in a campaign targeting Taiwan during Nancy Pelosi’s visit in August 2022. During this campaign, we observed Empire Dragon accounts sharing content first

[reported](#) by Graphika in September 2022. For example, we observed Empire Dragon accounts sharing posts using the string “mmexport1660466180684”, which Graphika also reported during the campaign targeting Taiwan; they had assessed that this string likely originated from default filenames for content downloaded from WeChat, a Chinese messaging platform. At the time, Graphika chose to keep the campaign unattributed despite “limited connections to the Spamouflage network”, which the firm considers as a distinct activity set to the network observed targeting Nancy Pelosi and Tsai Ing-Wen. Spamouflage (or Spamouflage Dragon) is a “[pro-Chinese propaganda network](#)” covered by Graphika since at least [2019](#).

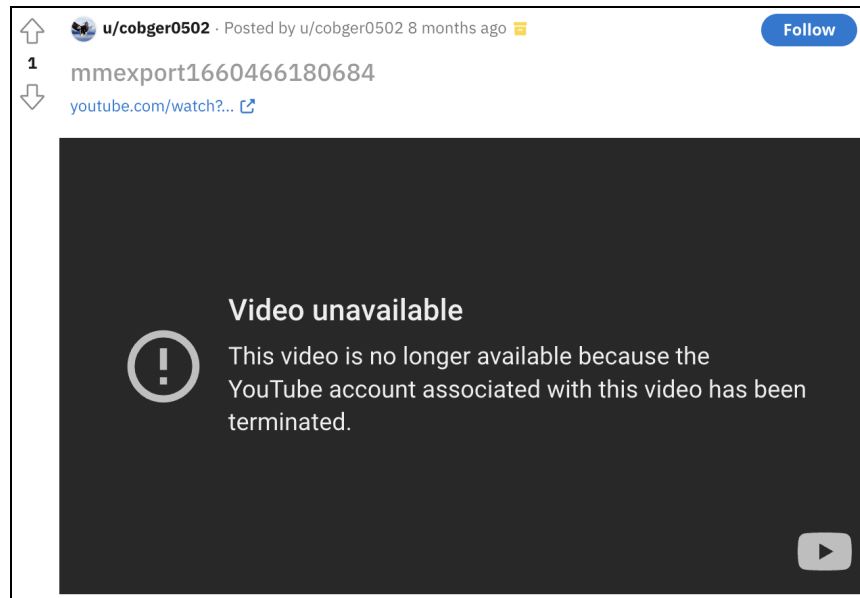


Figure 31: Video shared by an Empire Dragon account using a title previously observed by Graphika (Source: [Reddit](#))

We also observed a significant overlap between this network and DRAGONBRIDGE, a “pro-PRC influence campaign” [tracked](#) by Mandiant since 2019. Our observations included narrative and technical overlaps such as the amplification of Russian state narratives around the NordStream pipeline sabotage, the attribution of Chinese cyber-espionage groups to the US government, and narratives [targeting](#) Guo Wengui and Dr. Li-Meng Yan.

Empire Dragon’s IO accusing the US government of operating APT41 and other cyber-espionage groups was also attributed to a “cyber-enabled influence operation linked to the Spamouflage network” by ASPI in a report [published](#) in April 2023. Many of the TTPs, behavioral characteristics, and narratives described in ASPI’s report overlap with Empire Dragon activity, including the use of inauthentic accounts with Western personas, female profile pictures, and pattern-of-life analysis indicating activity concentrated in GMT+8 office hours.

Empire Dragon activity also overlaps with a pro-PRC “inauthentic online network” [reported](#) by Nisos in April 2023. The network was identified as spreading the same identical content as Empire Dragon accounts to target the US government in the context of the Ninth Review of the BWC. Nisos researchers also identified a post on a Chinese forum claiming that the specific operation was

conducted by “military bloggers inside and outside the wall” with ties to the [50 Cent Party](#), a known Chinese nationalist group accused of conducting domestic information operations. We were not able to identify further evidence supporting this claim.

Lastly, one of the NGOs attacked by Empire Dragon, Safeguard Defenders, published its own [findings](#) on accounts targeting the organization in May 2023 — which we attribute to Empire Dragon — in which it described being targeted in a “prolonged campaign” since September 2022. Many of the TTPs described in the report correspond to TTPs previously observed in other Empire Dragon operations, including the use of inauthentic accounts with Western personas, embedded text in videos, and copycat accounts imitating targets.

Tactics, Techniques, and Procedures

The TTPs used by Empire Dragon overlap with those reported by other vendors (see “Overlap With Previously Attributed Clusters”, above). This includes the use of accounts with inauthentic identities, including stolen profile pictures, account impersonation, usernames following similar naming conventions, and the use of embedded text in videos (such as screenshots or screen recordings of PDF documents). These techniques have helped us identify Empire Dragon as an inauthentic network following our assessment of coordination above.

Inauthentic Accounts

While a majority of Empire Dragon accounts have been observed using default platform profile pictures and non-descript images, we have also observed a significant portion of accounts using stolen profile pictures. These images (which more often than not used [female personas](#), a tactic previously covered by [Graphika](#)) were often found on several Chinese-language image-sharing websites, TikTok, and other Chinese-language social media platforms or blogs.



Figure 32: Profile picture used by an Empire Dragon inauthentic social media account (Source: [Social Media](#))



Figure 33: Reverse image search results for an Empire Dragon account (Source: Google)

Account Impersonation

On 2 separate occasions, security researchers and targeted entities identified coordinated campaigns impersonating targets' social media accounts, including [Intrusion Truth](#) and [Safeguard Defenders](#). These accounts typically used handles typosquatting targets' legitimate handles, stolen profile pictures, and identical descriptions to impersonate targets, which we assess were attempts at diverting social media traffic to these entities, both of whom are critical of the Chinese government.



Figure 34: Security researchers' identification of a suspected impersonation campaign targeting Intrusion Truth (Source: [Social Media](#))

Naming Conventions

We also identified early groups of Empire Dragon accounts with similar naming conventions, which often shared other indicators such as the accounts' registration dates and first post dates. Groups of accounts following [similar naming conventions](#) may indicate coordinated behavior. However, this is one indicator among many to consider when determining the inauthenticity of any given network.

For example, the cluster below of 6 accounts observed engaging in Empire Dragon operations all follow a similar naming convention (*8237), with several being nearly identical (ailawei8327, aisawei8327, and ainisiweier8237). All were registered on a single platform in 3 days between March 22 and 25, 2021. Although some of these accounts may have been registered on different days, 5 of these accounts authored posts for the first time on the same date a month later, on April 20, 2021.

Username	Account Creation Date	First Post Date
feinier8327	03-22-2021	03-25-2021
qiyiqiyi8327	03-23-2021	04-20-2021
ailawei8327	03-25-2021	04-20-2021
aisawei8327	03-25-2021	04-20-2021
ainisiweier8327	03-25-2021	04-20-2021
xuezhitianshi8327	03-25-2021	04-20-2021

Table 3: Account registration data following similar naming conventions (Source: Recorded Future)

Embedded Text in Videos

We identified several cases of Empire Dragon-related content being embedded as text in videos, which we assess is likely an attempt at evading detection. The text, which was often identical to content amplified by accounts on other platforms, was often featured as part of slideshows, or even as part of screen recordings of an operator scrolling through a PDF file.

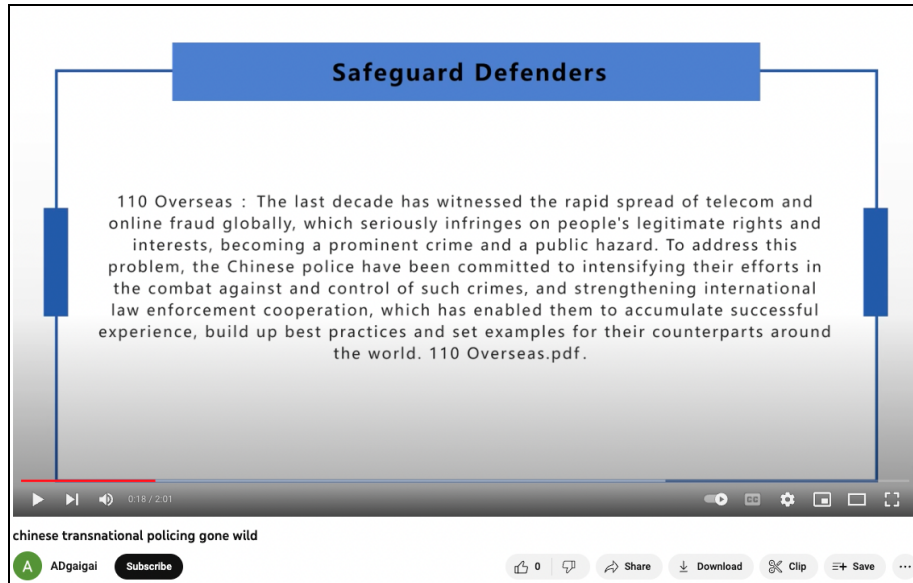


Figure 35: YouTube video shared by Empire Dragon accounts (Source: YouTube — page removed)

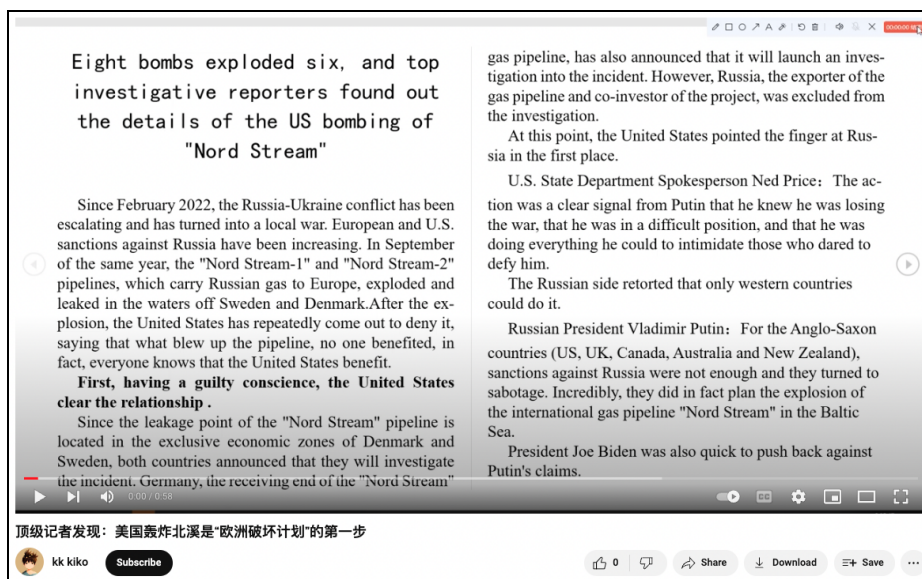


Figure 36: YouTube video shared by Empire Dragon accounts (Source: YouTube — page removed)

Outlook

Empire Dragon's shift toward tactical information operations likely demonstrates increased intent from Chinese government-aligned influence actors to use covert IO as an incisive tool to manipulate public opinion on current events, while retaining strategic operations targeting long-term adversaries of the state. Insikt Group assesses that this very likely signals the Chinese government's intent to continue scaling its use of coordinated inauthentic networks to amplify conspiracy theories, attack opponents, and discredit critics and that it will likely engage in covert information operations in the months leading up to the 2024 Taiwan and US presidential elections. These covert efforts will almost certainly be supported by China's well-established [ecosystem](#) of overt communications channels, which leverages state media and [civil servants](#)' social media presence. Likely targets include specific government departments, individual political leaders, international organizations, and NGOs.

The narrative convergence in IO between Russian and Chinese government-aligned influence actors observed in recent information operations conducted by Empire Dragon suggests that, despite different geopolitical objectives, we are observing a wider [convergence](#) in overt and covert influence activity from both countries. Covert information operations are the latest tool used by Chinese government-aligned influence actors to amplify [mutually beneficial](#) narratives in the face of US-led international governance and the [enlargement](#) of NATO following the Russian invasion of Ukraine.

Evidence presented in this report suggests that, beyond narratives, this convergence is also taking place at a tactical level, with an increased emphasis on tactical operations reacting to geopolitical events, amplifying emerging conspiracy theories, attacking international organizations, and co-opting Western "useful idiots" and fringe political groups to advance narratives undermining the US and promoting China. Chinese government-aligned networks like Empire Dragon have likely taken notes from their Russian counterparts and will more probably than not adopt other tactics seeing current use by Russian IO.

Empire Dragon's operations have generated very low levels of organic engagement by targeted audiences, which we attribute to limited investment or interest in developing quality content, the obvious recycling of identical image and text content, low-quality translations across languages, and a failure to covertly seed content using established influencers or sources. This impotence is likely to push China to look at how it can improve its playbook for using coordinated inauthentic networks as an effective tool to shape international discourse to its benefit, a topic of [strategic importance](#) to the CCP. As a result, we assess that the actors behind the network are likely in the process of iterating its TTPs while simultaneously scaling its operations and maintaining operational tempo. Content quality is likely to be improved with the advent of multilingual large language models (LLMs) and advanced image generation models, meaning that we will almost certainly witness an improvement in Western audiences' engagement with Chinese state-aligned IO despite linguistic and cultural barriers. As per previous Insikt Group findings, the Chinese government will also likely continue [tailoring](#) its influence efforts to targeted audiences using data analytics, group segmentation, and other "precise communication" techniques.

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,700 businesses and government organizations across more than 75 countries to provide real-time, unbiased and actionable intelligence. Learn more at [recordedfuture.com](https://www.recordedfuture.com).