Microsoft

Sophistication, scope, and scale:

Digital threats from East Asia increase in breadth and effectiveness

September 2023

Microsoft Threat Intelligence

Table of contents

3 **Introduction**

4 **Chinese cyber operations**

6 **Chinese influence operations**

6 CCP social media operations increase effective audience engagement

10 Chinese IO expands global reach in several campaigns

15 **North Korean cyber operations**

17 **Looking ahead**

Introduction

Several emerging trends illustrate a quickly changing threat landscape across East Asia, with China conducting both widespread cyber and influence operations (IO), and North Korean cyber threat actors demonstrating increased sophistication.

First, Chinese state-affiliated cyber threat groups have shown particular focus on the South China Sea region, directing cyber espionage at governments and other critical entities that ring this maritime area. Meanwhile, China's targeting of the US defense sector and probing of US infrastructure signals attempts to gain competitive advantages for China's foreign relations and strategic military aims.

Second, China has become more effective at engaging social media users with IO in the past year. Chinese online influence campaigns have long relied on sheer volume to reach users through networks of inauthentic social media accounts. Since 2022, however, China-aligned social media networks have engaged directly with authentic users on social media, targeted specific candidates in content about US elections, and posed as American voters. Separately, China's state-affiliated multilingual social media influencer initiative has successfully engaged target audiences in at least 40 languages and grown its audience to over 103 million.

Third, China has continued to scale up its IO campaigns in the past year, expanding efforts to new languages and new platforms to increase its global footprint. On social media, campaigns deploy thousands of inauthentic accounts across dozens of websites, spreading memes, videos, and messages in multiple languages. In online news media, Chinese state media is tactful and effective in positioning itself as the authoritative voice on international discourse on China, using a variety of means to exert influence in media outlets worldwide. One campaign pushed Chinese Communist Party (CCP) propaganda via localized news websites aimed at the Chinese diaspora in more than 35 countries.

Finally, North Korea—which, unlike China, lacks capability as a sophisticated influence actor—remains a formidable cyber threat. North Korea has shown a continued interest in intelligence collection and increasing tactical sophistication by leveraging cascading supply chain attacks and cryptocurrency theft, among other tactics.

Chinese cyber operations

China's cyber operations renew focus on South China Sea and key industries in the United States

Since the beginning of 2023, Microsoft Threat Intelligence has identified three areas of particular focus for China-affiliated cyber threat actors: the South China Sea, the US defense industrial base, and US critical infrastructure.

Chinese state-sponsored targeting mirrors strategic goals in the South China Sea

Chinese state-affiliated threat actors show continued interest in the South China Sea and Taiwan, which reflects China's wide range of economic, defense, and political interests in this region.[1] Conflicting territorial claims, rising cross-Strait tensions, and an increased US military presence may all be motivations for China's offensive cyber activities.[2]

Microsoft has tracked Raspberry Typhoon (RADIUM) as the primary threat group targeting nations that ring the South China Sea. Raspberry Typhoon consistently targets government ministries, military entities, and corporate entities connected to critical infrastructure, particularly telecoms. Since January 2023, Raspberry Typhoon has been particularly persistent. When targeting government ministries or infrastructure, Raspberry Typhoon typically conducts intelligence collection and malware execution. In many countries, targets vary from defense and intelligence-related ministries to economic and trade-related ministries.

Flax Typhoon (Storm-0919) is the most prominent threat group targeting the island of Taiwan. This group primarily targets telecommunications, education, information technology, and energy infrastructure, typically by leveraging a custom VPN appliance to directly establish a presence within the target network. Similarly, Charcoal Typhoon (CHROMIUM) targets Taiwanese education institutions, energy infrastructure, and high-tech manufacturing. In 2023, both Charcoal Typhoon and Flax Typhoon targeted Taiwanese aerospace entities that contract with the Taiwanese military.

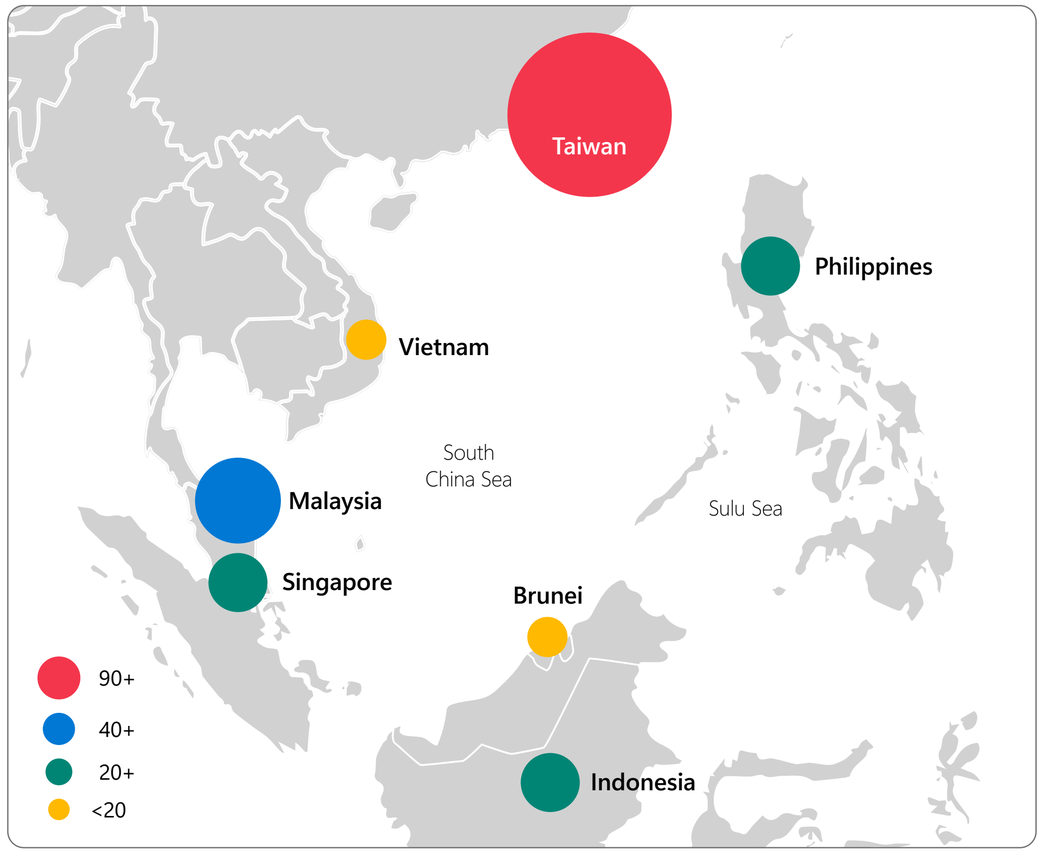


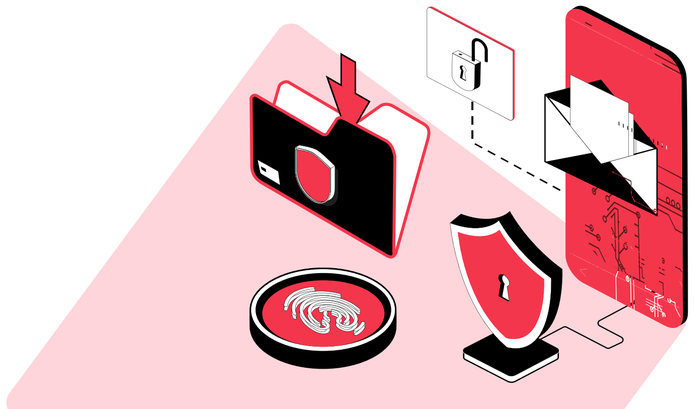
Figure 1: Observed events per country in the South China Sea from January 2022 to April 2023.

Chinese threat actors turn attention toward Guam as US builds a Marine Corps base

Multiple China-based threat groups continue to target the US defense industrial base, namely Circle Typhoon (DEV-0322), Volt Typhoon (DEV-0391), and Mulberry Typhoon (MANGANESE). While the targets of these three groups occasionally overlap, they are distinct actors with different infrastructure and capabilities.[3]

Circle Typhoon conducts a wide range of cyber activity against the US defense industrial base including resource development, collection, initial access, and credential access. Circle Typhoon often leverages VPN appliances to target IT and US-based defense contractors. Volt Typhoon has also conducted reconnaissance against numerous US defense contractors. Guam is one of the most frequent targets of these campaigns, particularly the satellite communications and telecommunications entities housed there.[4]

A frequent tactic of Volt Typhoon involves compromising small office and home routers, typically for the purpose of building infrastructure.[5] Mulberry Typhoon has also targeted the US defense industrial base, most notably with a zero-day exploit targeting devices.[6] Increased targeting of Guam is significant given its position as the closest US territory to East Asia and crucial to US strategy in the region.



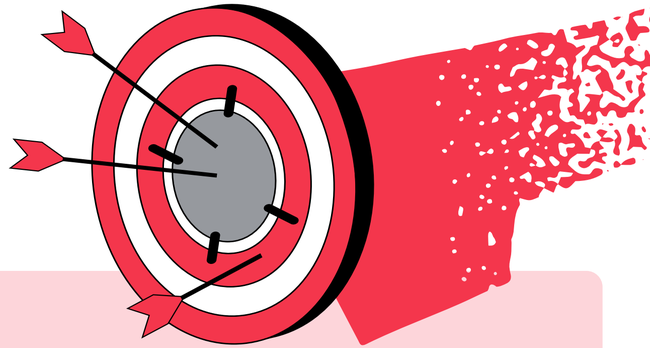
Chinese threat groups target US critical infrastructure

Microsoft has observed Chinese state-affiliated threat groups targeting US critical infrastructure across multiple sectors and significant resource development over the last six months. Volt Typhoon has been the primary group behind this activity since at least the summer of 2021, and the extent of this activity is still not fully known.

Targeted sectors include transportation (such as ports and rail), utilities (such as energy and water treatment), medical infrastructure (including hospitals), and telecommunications infrastructure (including satellite communications and fiber optic systems). Microsoft assesses that this campaign could provide China with capabilities to disrupt critical infrastructure and communications between the United States and Asia.[7]

China-based threat group targets approximately 25 organizations including US government entities

Beginning May 15, Storm-0558, a China-based threat actor, used forged authentication tokens to access Microsoft customer email accounts of approximately 25 organizations, including US and European government entities.[8] Microsoft has successfully blocked this campaign. The objective of the attack was to obtain unauthorized access to email accounts. Microsoft assesses this activity was consistent with Storm-0558's espionage objectives. Storm-0558 has previously targeted US and European diplomatic entities.



China also targets its strategic partners

As China has grown its bilateral relations and global partnerships through the Belt and Road Initiative (BRI), Chinese state-affiliated threat actors have conducted parallel cyber operations against private and public entities around the world. China-based threat groups target countries that are in line with the CCP's BRI strategy, including entities in Kazakhstan, Namibia, Vietnam, and more.[9] Meanwhile, widespread Chinese threat activity consistently targets foreign ministries based throughout Europe, Latin America, and Asia—likely in pursuit of economic espionage or intelligence collection objectives.[10] As China expands its global influence, affiliated threat groups' activities are to follow. As recently as April 2023, Twill Typhoon (TANTALUM) successfully compromised government machines in Africa and Europe as well as humanitarian organizations worldwide.

Chinese influence operations

CCP-aligned social media operations increase effective audience engagement

Figure 2: A Black Lives Matter graphic first uploaded by a CCP-affiliated automated account was then uploaded by an account impersonating a US conservative voter seven hours later.

CCP-affiliated covert influence operations have now begun to successfully engage with target audiences on social media to a greater extent than previously observed, representing higher levels of sophistication and cultivation of online IO assets. Ahead of the 2022 US midterms, Microsoft and industry partners observed CCP-affiliated social media accounts impersonating US voters—new territory for CCP-affiliated IO.[11] These accounts posed as Americans across the political spectrum and responded to comments from authentic users.

In both behavior and content, these accounts display many well-documented Chinese IO tactics, techniques, and procedures (TTPs). Examples include: accounts posting in Mandarin in their early stages before switching to another language, engaging with content from other China-aligned assets immediately after posting, and using a "seed and amplifier" pattern of interaction.[12] Unlike earlier IO campaigns from CCP-affiliated actors that used easy-to-spot computer-generated handles, display names and profile pictures,[13] these more sophisticated accounts are operated by real people who employ fictitious or stolen identities to conceal the accounts' affiliation with the CCP.

Social media accounts in this network show similar behavior to activity reportedly conducted by an elite group within the Ministry of Public Security (MPS) called the 912 Special Working Group. According to the US Department of Justice, the group operated a social media troll farm that created thousands of fake online personas and pushed CCP propaganda targeting pro-democracy activists.

Since approximately March 2023, some suspected Chinese IO assets on Western social media have begun to leverage generative artificial intelligence (AI) to create visual content. This relatively high-quality visual content has already drawn higher levels of engagement from authentic social media users. These images bear the hallmarks of diffusion-powered image generation and are more eye-catching than awkward visual content in previous campaigns. Users have more frequently reposted these visuals, despite common indicators of AI-generation—for example, more than five fingers on a person's hand.[14]

Figure 3: Example of an AI-generated image posted by a suspected Chinese IO asset. The Statue of Liberty's hand holding the torch has more than five fingers.

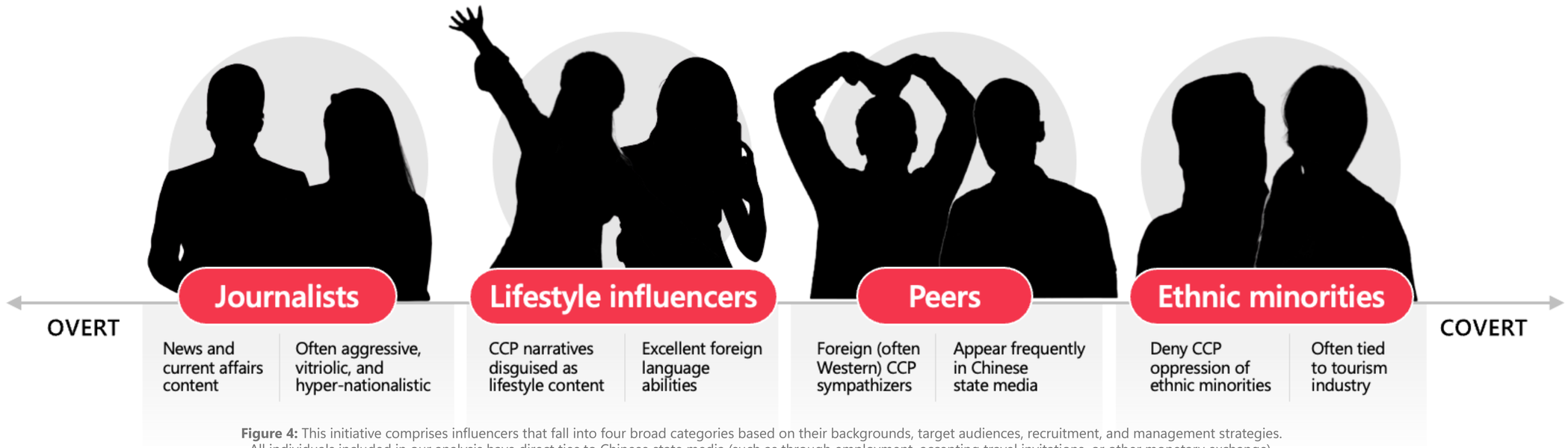


Figure 4: This initiative comprises influencers that fall into four broad categories based on their backgrounds, target audiences, recruitment, and management strategies. All individuals included in our analysis have direct ties to Chinese state media (such as through employment, accepting travel invitations, or other monetary exchange).

The Chinese state media influencer initiative

Another strategy drawing meaningful engagement on social media is the CCP's concept of "multilingual internet celebrity studios" (多语种网红工作室).[15] Leveraging the power of authentic voices, more than 230 state media employees and affiliates masquerade as independent social media influencers across all major Western social media platforms.[16] In 2022 and 2023, new influencers continue to debut every seven weeks on average. Recruited, trained, promoted, and funded by China Radio International (CRI) and other Chinese state media outfits, these influencers spread expertly localized CCP propaganda that achieves meaningful engagement with target audiences around the world, reaching a combined following of at least 103 million across multiple platforms speaking at least 40 languages.

Although influencers post mostly innocuous lifestyle content, this technique disguises CCP-aligned propaganda that seeks to soften China's image abroad.

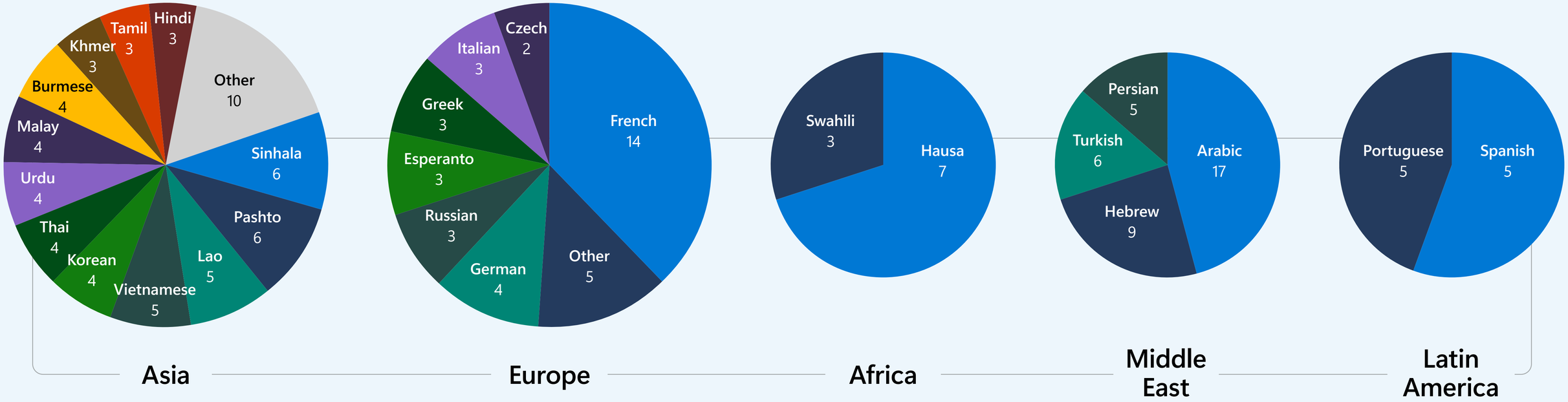
Chinese state media's influencer recruitment strategy appears to enlist two distinct groups of individuals: those with experience working in journalism (at state media outlets specifically), and recent graduates of foreign language programs. In particular, China Media Group (the parent company of CRI and CGTN) appears to directly recruit graduates of top Chinese foreign language schools like Beijing Foreign Studies University and the Communication University of China. Those who are not directly recruited from universities are often former journalists and translators, who remove any explicit indicators of state media affiliation from their profiles after "rebranding" as influencers.

Figure 5: Lao-speaking influencer Song Siao posts a lifestyle vlog discussing China's economic recovery amidst the COVID-19 pandemic. In the self-filmed video, he visits a car dealership in Beijing and speaks with locals.

Figure 6: Techy Rachel, an English-language influencer who typically posts about Chinese innovations and technology, deviates from her content themes to weigh in on the Chinese spy balloon debate. Like other Chinese state media outlets, she denies that the balloon was used for espionage.

Influencers reach worldwide audiences in at least 40 languages

The geographic distribution of languages spoken by these state-affiliated influencers represents China's growing global influence and regional prioritization. Influencers speaking Asian languages excluding Chinese—such as Hindi, Sinhala, Pashto, Lao, Korean, Malay, and Vietnamese—comprise the largest number of influencers. English-speaking influencers make up the second-highest number of influencers.



China targeting audiences worldwide

Influencers target seven audience spaces (language groupings) that are separated into geographic region. No charts shown for English or Chinese-language audience spaces.

Figure 7: Chinese state media influencers breakdown by language.

Chinese IO expands global reach in several campaigns

China further expanded the scale of its online IO in 2023 by reaching audiences in new languages and on new platforms. These operations combine a highly controlled overt state media apparatus with covert or obfuscated social media assets, including bots, that launder and amplify the CCP's preferred narratives.[17]

Microsoft observed one such CCP-aligned campaign, beginning in January 2022 and ongoing at the time of this writing, targeting Spanish non-governmental organization (NGO) Safeguard Defenders after it exposed the existence of more than 50 overseas Chinese police stations.[18] This campaign deployed more than 1,800 accounts across several social media platforms and dozens of websites to spread CCP-aligned memes, videos, and messages that criticized the United States and other democracies. These accounts messaged in new languages (Dutch, Greek, Indonesian, Swedish, Turkish, Uyghur, and more) and on new platforms (including Fandango, Rotten Tomatoes, Medium, Chess.com, and VK, among others). Despite the scale and persistence of this operation, its posts rarely garner meaningful engagement from authentic users, highlighting the rudimentary nature of these Chinese networks' activity.

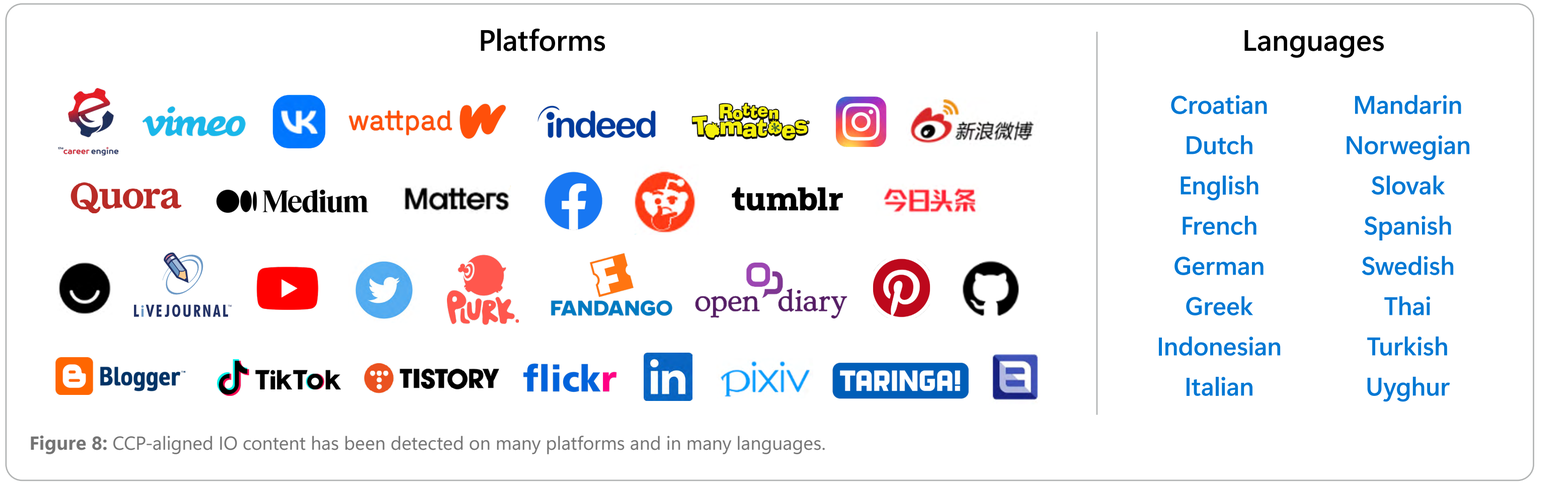


Figure 8: CCP-aligned IO content has been detected on many platforms and in many languages.

Figure 9: High-volume shares of posts of a Taiwanese-language video calling on the Taiwanese government to "surrender" to Beijing. The large difference between impressions and shares is highly indicative of coordinated IO activity.

A veiled global network of CCP news websites

Another digital media campaign that illustrates the expanded breadth of CCP-affiliated IO is a network of more than 50 predominately Chinese-language news websites that support the CCP's stated goal of being the authoritative voice of all Chinese-language media worldwide.[19] Despite presenting as largely independent, unaffiliated websites catering to different Chinese diaspora communities around the globe, we assess with high confidence that these websites are affiliated with the CCP's United Front Work Department (UFWD)—an organ responsible for strengthening the CCP's influence beyond China's borders: particularly by liaising with "overseas Chinese"—based on technical indicators, website registration information, and shared content.[20]

Figure 10: Map of websites targeting the global Chinese diaspora that are assessed to be part of this media strategy.

Because many of these sites share IP addresses, querying domain resolutions with Microsoft Defender Threat Intelligence allowed us to discover more sites in the network. Many of the websites share front-end web HTML code, in which even the web developer comments embedded in the code are often identical across different websites. More than 30 of the sites leverage the same application programming interface (API) and content management system from a "wholly-owned subsidiary" of China News Service (CNS), the UFWD's media agency.[21] Records from China's Ministry of Industry and Information Technology further reveal that this UFWD-affiliated tech company and another have registered at least 14 news sites in this network.[22] By using subsidiaries and third-party media companies in this way, the UFWD can reach a global audience while obscuring its direct involvement.

These websites purport to be independent news providers while frequently republishing the same Chinese state media articles, often claiming to be the original source of the content. While the sites broadly cover international news and publish generic Chinese state media articles, politically sensitive subjects overwhelmingly align with the CCP's preferred narratives. For example, several hundred articles within this network of websites promote false claims that the COVID-19 virus is a bioweapon manufactured at the US military biological research laboratory at Fort Detrick.[23] Sites also frequently circulate statements from Chinese government officials and state media articles alleging the COVID-19 virus originated in the United States and not in China. These websites exemplify the extent to which CCP control has permeated the Chinese-language media environment, allowing the Party to drown out critical reporting of sensitive subjects.

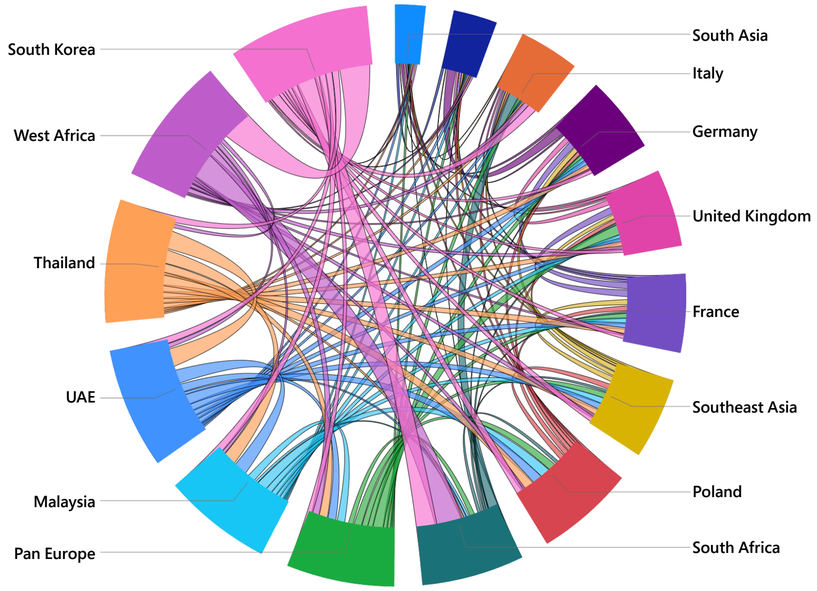
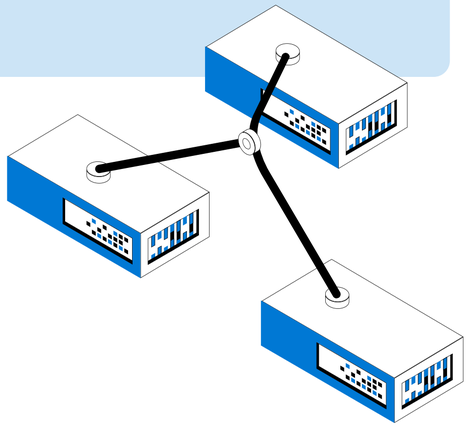


Figure 11: Websites present as unique to locality but share identical content. This chord diagram shows overlapping articles published by multiple sites.

Figure 12: China News Service and other Chinese state media published an article titled "Statement from the WHO exposes dark US biolaboratories in Ukraine." This article was then published across websites targeting audiences in Hungary, Sweden, West Africa, and Greece.

Chinese state media's global reach

While the campaign described above is notable for its obfuscation, bona fide Chinese state media websites account for the vast majority of global viewership of CCP-directed media. By expanding into foreign languages,[24] opening Chinese state media bureaus abroad,[25] and supplying free Beijing-friendly content,[26] the CCP extends the reach of its "discourse power" (话语权) by injecting propaganda into the news media of countries around the world.[27]



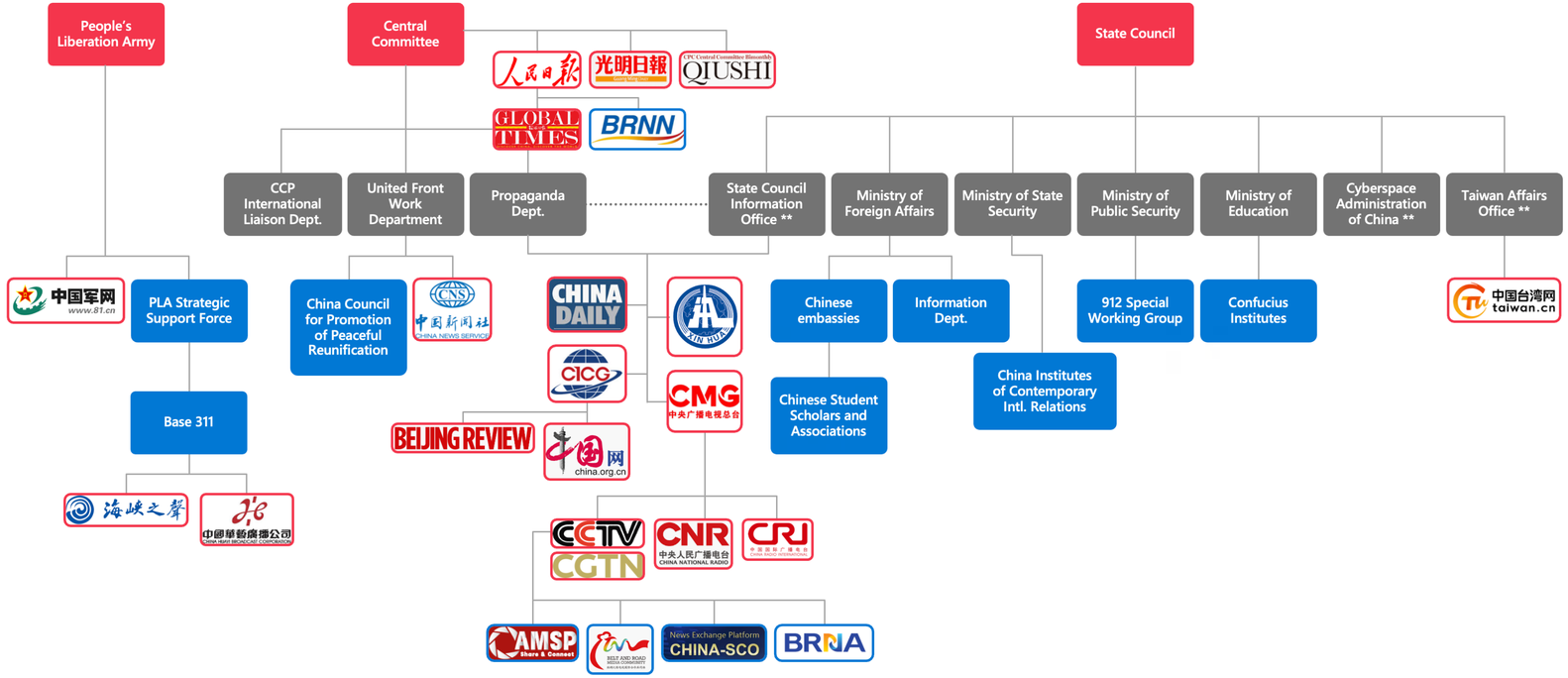


Figure 13: Organizational chart representing a snapshot of the functions and entities forming part of the CCP's overt propaganda ecosystem.

Measuring traffic to Chinese state media websites

Microsoft's AI for Good Lab has developed an index to measure the flow of traffic from users outside China to outlets majority-owned by the Chinese government. The index measures the proportion of traffic visiting these sites to overall traffic on the internet, like the Russian Propaganda Index (RPI) introduced in June 2022.[28]

Five domains dominate consumption of Chinese state media, accounting for approximately 60% of all Chinese state media page views.

32% **Phoenix TV**
ifeng.com
Chinese government-owned Bauhinia Culture acquired a majority stake of Phoenix TV (凤凰卫视) in 2021.[29]

11% **People's Daily**
people.com.cn
People's Daily (人民日报) is the official newspaper of the CCP's Central Committee.

7% **Huanqiu**
huanqiu.com
Huanqiu (环球) is a state outlet under People's Daily.

5% **Xuexi Qiangguo**
xuexi.cn
Xuexi Qiangguo (学习强国) is a website and application designed to promote "Xi Jinping Thought."[30]

4% **The Paper**
thepaper.cn
The Paper (澎湃新闻) is owned and run by state media company Shanghai United Media Group.[31]

The above data is drawn from January to April 2023.

The index can illuminate trends in the relative success of Chinese state media outlets by geography over time. For instance, among Association of Southeast Asian Nations (ASEAN) member states, Singapore and Laos stand out with more than twice the relative traffic to Chinese state media websites as third-ranked Brunei. The Philippines ranks lowest, with 30x less traffic to Chinese state media websites than Singapore and Laos. In Singapore, where Mandarin is an official language, high consumption of Chinese state media reflects China's influence on Mandarin-language news. In Laos, Chinese speakers number far fewer, which reflects the relative success of Chinese state media in the country's environment.

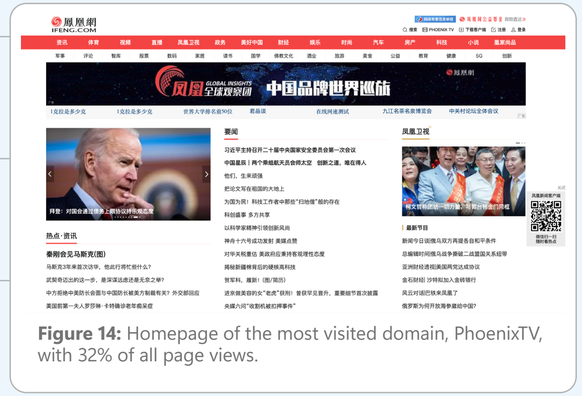


Figure 14: Homepage of the most visited domain, PhoenixTV, with 32% of all page views.

North Korean cyber operations

Increasingly sophisticated North Korean cyber operations collect intelligence and generate revenue for the state

North Korean cyber threat actors pursue cyber operations aiming to (1) collect intelligence on the activities of the state's perceived adversaries: South Korea, the United States, and Japan, (2) collect intelligence on other countries' military capabilities to improve their own, and (3) collect cryptocurrency funds for the state. Over the past year, Microsoft observed greater targeting overlaps among distinct North Korean threat actors and an increase in the sophistication of North Korean activity groups.

North Korea's cyber priorities emphasize maritime technology research amidst testing of underwater drones and vehicles

Over the past year, Microsoft Threat Intelligence has observed greater targeting overlaps across North Korean threat actors. For example, three North Korean threat actors—Ruby Sleet (CERIUM), Diamond Sleet (ZINC), and Sapphire Sleet (COPERNICIUM)—targeted the maritime and shipbuilding sector from November 2022 to January 2023. Microsoft had not previously observed this level of targeting overlaps across multiple North Korean activity groups, suggesting that maritime technology research was a high priority for the North Korean government at the time. In March 2023, North Korea reportedly test-fired two strategic cruise missiles from a submarine towards the Sea of Japan (a.k.a. East Sea) as a warning ahead of the South Korea-US Freedom Shield military exercise. Later that month and the following, North Korea allegedly tested two Haeil underwater attack drones off the country's east coast towards the Sea of Japan. These maritime military capabilities tests occurred shortly after three North Korean cyber groups targeted maritime defense entities for intelligence collection.

Threat actors compromise defense firms as North Korean regime sets high-priority collection requirements

From November 2022 to January 2023, Microsoft observed a second instance of targeting overlaps, with Ruby Sleet and Diamond Sleet compromising defense firms. The two threat actors compromised two arms manufacturing companies based in Germany and Israel. This suggests that the North Korean government is assigning multiple threat actor groups at once to meet high-priority collection requirements to improve the country's military capabilities. Since January 2023, Diamond Sleet has also compromised defense companies in Brazil, Czechia, Finland, Italy, Norway, and Poland.

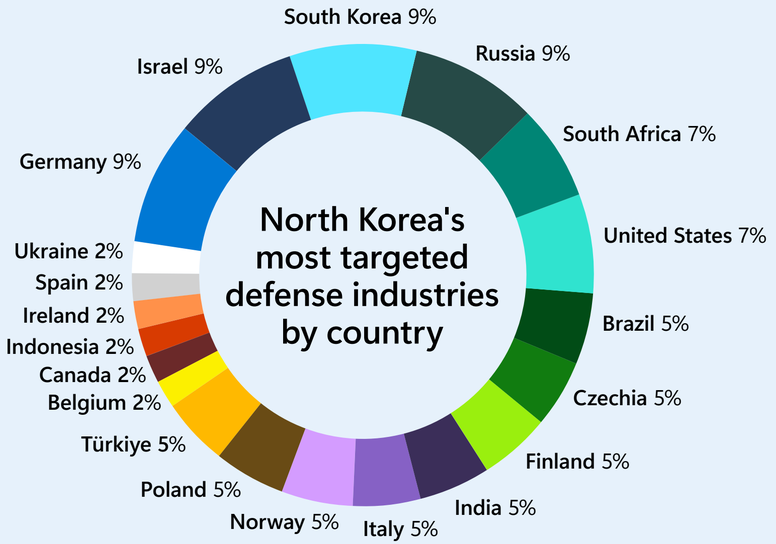


Figure 15: North Korea targeting defense industry by country, from March 2022 to March 2023.

Russian government and defense industries remain targets for North Korea to conduct intelligence collection

Multiple North Korean threat actors have recently targeted the Russian government and defense industry, while simultaneously providing materiel support for Russia in its war in Ukraine.[32] In March 2023, Ruby Sleet compromised an aerospace research institute in Russia. Additionally, Onyx Sleet (PLUTONIUM) compromised a device belonging to a university in Russia in early March. Separately, an attacker account attributed to Opal Sleet (OSMIUM) sent phishing emails to accounts belonging to Russian diplomatic government entities during the same month. North Korean threat actors may be capitalizing on the opportunity to conduct intelligence collection on Russian entities due to the country's focus on its war in Ukraine.

North Korean groups exhibit more sophisticated operations through cryptocurrency theft and supply chain attacks

Microsoft assesses that North Korean activity groups are conducting increasingly sophisticated operations through cryptocurrency theft and supply chain attacks. In January 2023, the Federal Bureau of Investigation (FBI) publicly attributed the June 2022 theft of $100 million in cryptocurrency from Harmony's Horizon Bridge to Jade Sleet (DEV-0954), a.k.a. Lazarus Group/APT38.[33] Furthermore, Microsoft attributed the March 2023 3CX supply chain attack that leveraged a prior supply chain compromise of a US-based financial technology company in 2022 to Citrine Sleet (DEV-0139). This was the first time Microsoft has observed an activity group using an existing supply chain compromise to conduct another supply chain attack, which demonstrates the increasing sophistication of North Korean cyber operations.

Emerald Sleet deploys tried-and-true spearphishing tactic by luring experts into replying with foreign policy insights

Emerald Sleet (THALLIUM) remains the most active North Korean threat actor Microsoft tracked over the past year. Emerald Sleet continues to send frequent spearphishing emails to Korean Peninsula experts around the world for intelligence collection purposes. In December 2022, Microsoft Threat Intelligence detailed Emerald Sleet's phishing campaigns targeting influential North Korea experts in the United States and US-allied countries. Rather than deploying malicious files or links to malicious websites, Microsoft found that Emerald Sleet employs a unique tactic: impersonating reputable academic institutions and NGOs to lure victims into replying with expert insights and commentary about foreign policies related to North Korea.

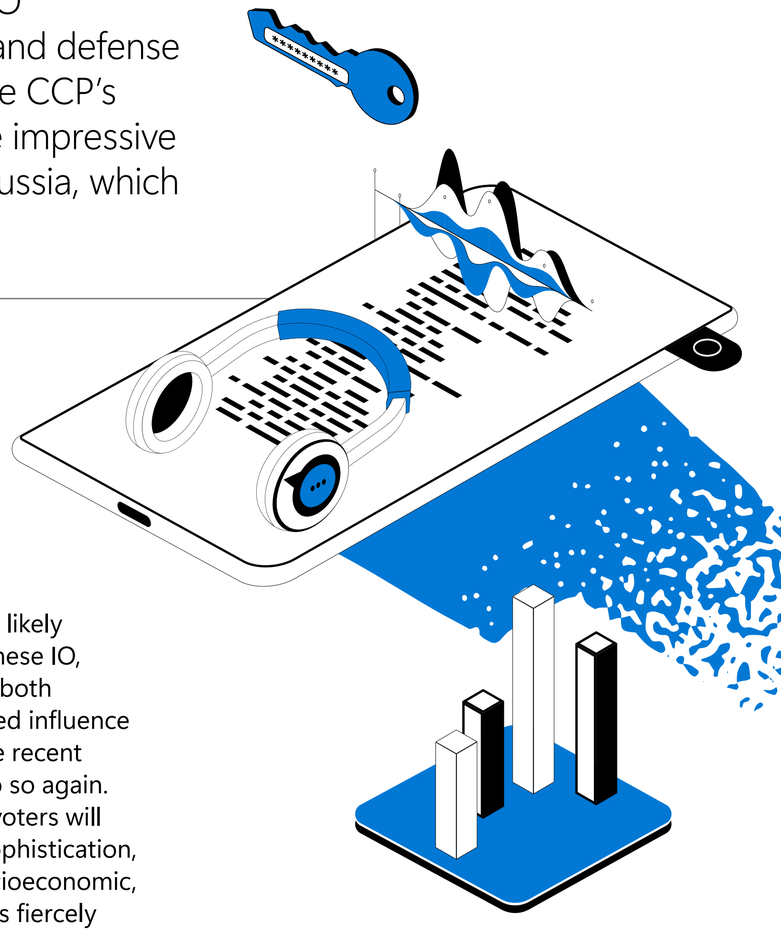
Capabilities: Influence

North Korea has conducted limited influence operations on video-sharing social media platforms like YouTube and TikTok over the past year.[34] North Korean influencers on YouTube are mostly girls and women, one as young as eleven years old, who post vlogs about their daily lives and promote positive narratives about the regime. Some of the influencers speak English in their videos, intending to reach a wider global audience. North Korea's influencers are much less effective than the Chinese state media-backed influencer initiative.

Looking ahead

Looking ahead as geopolitical tensions charge cyber activity and influence operations

China has continued to expand its cyber capabilities in recent years and shown much more ambition in its IO campaigns. In the near term, North Korea is to remain focused on targets related to its political, economic, and defense interests in the region. We can expect wider cyber espionage against both opponents and supporters of the CCP's geopolitical objectives on every continent. While China-based threat groups continue to develop and utilize impressive cyber capabilities, we have not observed China combine cyber and influence operations—unlike Iran and Russia, which engage in hack-and-leak campaigns.



Operating at a scale unmatched by other malign influence actors, China-aligned influence actors are poised to capitalize on several key trends and events over the next six months.

1

First, operations making use of video and visual media are becoming the norm. CCP-affiliated networks have long utilized AI-generated profile pictures, and this year have adopted AI-generated art for visual memes. State-backed actors will also continue to tap private content studios and public relations firms to outsource propaganda on demand.[35]

2

Second, China will continue to seek authentic audience engagement, investing time and resources into cultivated social media assets. Influencers with deep cultural and linguistic knowledge and high-quality video content have been pioneers for successful social media engagement. The CCP will apply some of these tactics, including interacting with social media users and demonstrating cultural know-how, to bolster its covert social media campaigns.

3

Third, Taiwan and the United States are likely to remain the top two priorities for Chinese IO, particularly with upcoming elections in both countries in 2024. Given that CCP-aligned influence actors have targeted US elections in the recent past, it is nearly certain that they will do so again. Social media assets impersonating US voters will likely demonstrate higher degrees of sophistication, actively sowing discord along racial, socioeconomic, and ideological lines with content that is fiercely critical of the United States.

1. cbsnews.com/news/china-us-philippines-military-bases-taiwan-tension-south-china-sea/; cfr.org/global-conflict-tracker/conflict/territorial-disputes-south-china-sea; www.state.gov/briefings-foreign-press-centers/chinas-maritime-claims-in-the-south-china-sea
2. New bases in the Philippines increase US military presence in the region, bbc.com/news/world-asia-64479712
3. At present there is insufficient evidence to tie the groups together.
4. wsj.com/articles/new-u-s-base-on-guam-is-aimed-at-deterring-china-11674731857
5. microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/
6. CVE-2022-27518; support.citrix.com/article/CTX474995/citrix-adc-and-citrix-gateway-security-bulletin-for-cve202227518; nvd.nist.gov/vuln/detail/CVE-2022-27518
7. microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/
8. microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/
9. query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE5bUvv?culture=en-us&country=us
10. microsoft.com/en-us/security/blog/2021/12/06/nickel-targeting-government-organizations-across-latin-america-and-europe/
11. about.fb.com/news/2022/09/removing-coordinated-inauthentic-behavior-from-china-and-russia/; foreignpolicy.com/2022/11/04/china-us-midterm-election-interference-meddling-social-media-cybersecurity-disinformation/; apnews.com/article/russia-ukraine-business-north-korea-e6a068d91bc9828ecadfb67c929a4162
12. miburo.substack.com/i/45539420/seeds-and-sprout
13. public-assets.graphika.com/reports/graphika_report_spamouflage_goes_to_america.pdf
14. washingtonpost.com/technology/2023/03/26/ai-generated-hands-midjourney/
15. archive.ph/QXvtw
16. miburo.substack.com/p/csm-influencer-ops-1; miburo.substack.com/p/chinese-state-medias-global-influencer; These statistics reflect data as of April 2023.
17. miburo.substack.com/p/spamouflage-survives; iri.org/wp-content/uploads/legacy/iri.org/detecting_digital_fingerprints__tracing_chinese_disinformation_in_taiwan_0.pdf; Such influence actors are sometimes known as "Spamouflage Dragon" or "DRAGONBRIDGE".
18. safeguarddefenders.com/en/blog/230000-policing-expands; safeguarddefenders.com/en/blog/patrol-and-persuade-follow-110-overseas-investigation
19. web.archive.org/web/20200527103611/media.people.com.cn/GB/40606/6198886.html
20. See: The Microsoft Threat Analysis Center's framework for determining influence attributions. blogs.microsoft.com/wp-content/uploads/prod/sites/5/2023/02/DTAC-Attribution-Framework.pdf; The Chinese diaspora is commonly referred to as "overseas Chinese" or 华侨 (huaqiao) by the Chinese government, referring to those with Chinese citizenship or heritage who reside outside of the PRC. For more detail on Beijing's interpretation of the Chinese diaspora, see: www.jstor.org/stable/26492596.
21. archive.ph/GWW0D
22. archive.is/oAn4j
23. The Chinese government seeded this narrative at the beginning of the COVID-19 pandemic, see: apnews.com/article/pandemics-beijing-only-on-ap-epidemics-media-122b73e134b780919cc1808f3f6f16e8. Websites within this network that promote this claim include: archive.ph/ueq4R; archive.ph/5DLGc; archive.ph/xmp6W.
24. economist.com/china/2018/06/14/china-is-spending-billions-on-its-foreign-language-media
25. foreignpolicy.com/2023/03/16/china-propaganda-africa-soft-power/
26. freedomhouse.org/report/beijing-global-media-influence/2022/authoritarian-expansion-power-democratic-resilience
27. digichina.stanford.edu/work/lexicon-discourse-power-or-the-right-to-speak-huayu-quan/
28. Defending Ukraine: Early Lessons from the Cyber War, query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK
29. web.archive.org/web/20210525192516/www.scmp.com/business/companies/article/3130027/phoenix-media-founder-sells-almost-all-his-shares-beijing-backed
30. Another interpretation of xuexi qiangguo is "Study Xi, Strengthen the Country." The name is a pun on Xi Jinping's family name. Governments, universities, and businesses in China strongly promote the use of the app, at times shaming or punishing subordinates for infrequent use, see: nytimes.com/2019/04/07/world/asia/china-xi-jinping-study-the-great-nation-app.html
31. The Paper is owned by Shanghai United Media Group, which is in turn owned by the Shanghai Communist Party Committee: nytimes.com/2016/04/06/business/international/china-media-the-paper-english.html
32. apnews.com/article/russia-ukraine-business-north-korea-e6a068d91bc9828ecadfb67c929a4162
33. fbi.gov/news/press-releases/fbi-confirms-lazarus-group-cyber-actors-responsible-for-harmonys-horizon-bridge-currency-theft
34. edition.cnn.com/2023/02/04/asia/north-korea-youtuber-yumi-intl-hnk-dst; tiktok.com/@viceworldnews/video/7190073973739179269
35. The CCP has previously invested in private sector companies that aid IO campaigns via SEO manipulation techniques, fake likes and followers, and other services. Procurement documents reveal such bids, see: www.nytimes.com/interactive/2021/12/20/technology/china-facebook-twitter-influence-manipulation.html