Pro-PRC "HaiEnergy" Information Operations Campaign Leverages Infrastructure from Public Relations Firm to Disseminate Content on Inauthentic News Sites

M **mandiant.com**/resources/pro-prc-information-operations-campaign-haienergy

Mandiant has identified an ongoing information operations (IO) campaign leveraging a network of at least 72 suspected inauthentic news sites and a number of suspected inauthentic social media assets to disseminate content strategically aligned with the political interests of the People's Republic of China (PRC). The sites present themselves primarily as independent news outlets from different regions across the world and publish content in 11 languages (see Appendix). Based on technical indicators we detail in this blog, we believe these sites are linked to Shanghai Haixun Technology Co., Ltd (上海海讯社科技有限公司), a Chinese public relations (PR) firm (referred to hereafter as "Haixun").

Narratives promoted by the campaign criticize the U.S. and its allies, attempt to reshape the international image of Xinjiang due to mounting international scrutiny, and express support for the reform of Hong Kong's electoral system—a change which gave the PRC more power over vetting local candidates. In addition to these broader themes, the campaign leveraged fabricated content designed to discredit opponents who have been critical of the Chinese Government, including Chinese businessman Guo Wengui (Miles Kwok) and German anthropologist Adrian Zenz—known for his research on Xinjiang—and China's reported genocide against the Uyghur population.

Given the distinctive tactics, techniques, and procedures (TTPs) employed by this campaign, we are classifying this activity set as its own campaign, which we have dubbed "HaiEnergy"—stemming from the campaign's use of infrastructure attributed to Haixun and services advertised by the PR firm as "positive energy packages." Notably, the term "positive energy" (正能量) is an important term in the Xi Jinping era that refers to messages positively portraying the Chinese Communist Party (CCP), the Chinese Government, and its policies.

Despite the capabilities and global reach of this campaign, there is at least some evidence to suggest that HaiEnergy failed to generate substantial engagement outside of the inauthentic amplification that we have identified—a limitation we also noted in our recent public reporting on DRAGONBRIDGE. We find the campaign's use of infrastructure linked to Haixun to be more interesting, as it is suggestive of recent trends surrounding the outsourcing of IO to third parties, which can make IO more accessible and help obfuscate the identities of an actor.

Infrastructure Linked to Shanghai Haixun Technology Co., Ltd (上海海讯社科技有限公司)

Based on information from public descriptions of the company's services, Haixun offers content creation and marketing services in at least 40 different languages in over 100 countries. Among their most notable offerings are the "Europe and U.S. Positive Energy" package, which includes content creation ostensibly geared towards English-speaking audiences, and the "Positive Energy Project Edition," which focuses on the production of tailor-made videos, promotion of custom content through "high-quality media resources," and campaign impact monitoring (Figure 1).
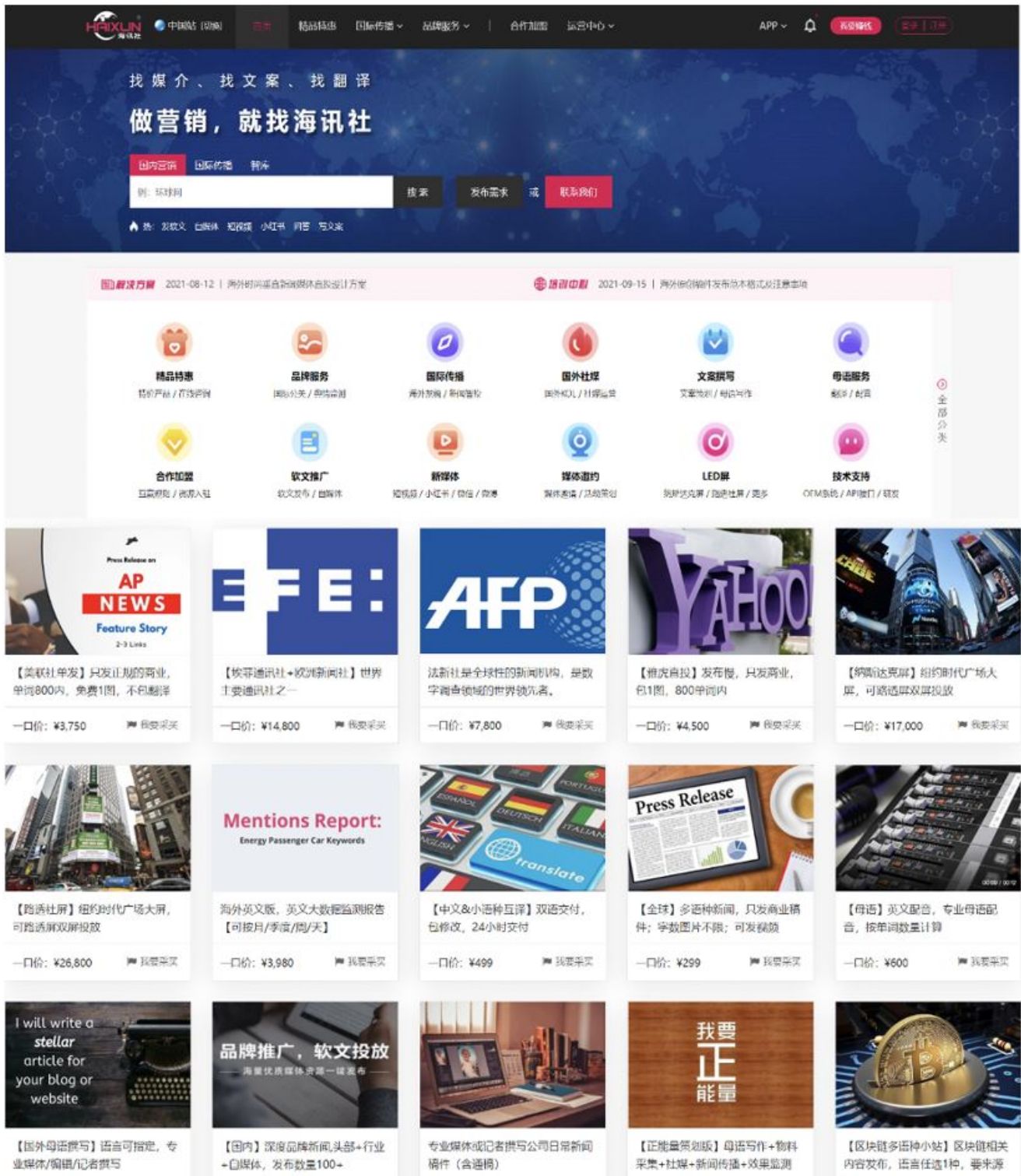
Figure 1: Haixun website offers a variety of "packages," including Positive Energy

While we do not currently have sufficient evidence to determine the extent to which Haixun is involved in, or even aware of HaiEnergy, our analysis indicates that the campaign has at least leveraged services and infrastructure belonging to Haixun to host and distribute content. In total, we identified 72 websites (59 domains and 13 subdomains) hosted by Haixun, which were used to target audiences in North America, Europe, the Middle East, and Asia.

- Sites attributed to HaiEnergy all display images and videos that are hosted on the server 02100.vip, which is registered by Haixun (Figure 2). Based on infrastructure overlap, we identified two additional domains (haixunpr.com and haixunpr.org)—Chinese- and English-language sites describing Haixun's services—that have resolved to the same IP address and leveraged content from 02100.vip.
- We observed multiple inauthentic news sites we attribute to "HaiEnergy" listed in a downloadable spreadsheet hosted at haixunpr.org. The spreadsheet features Chinese and Russian text and appears to be a distribution list for content (Figure 3). We note that the spreadsheet is no longer available to download as of the date of this publication.
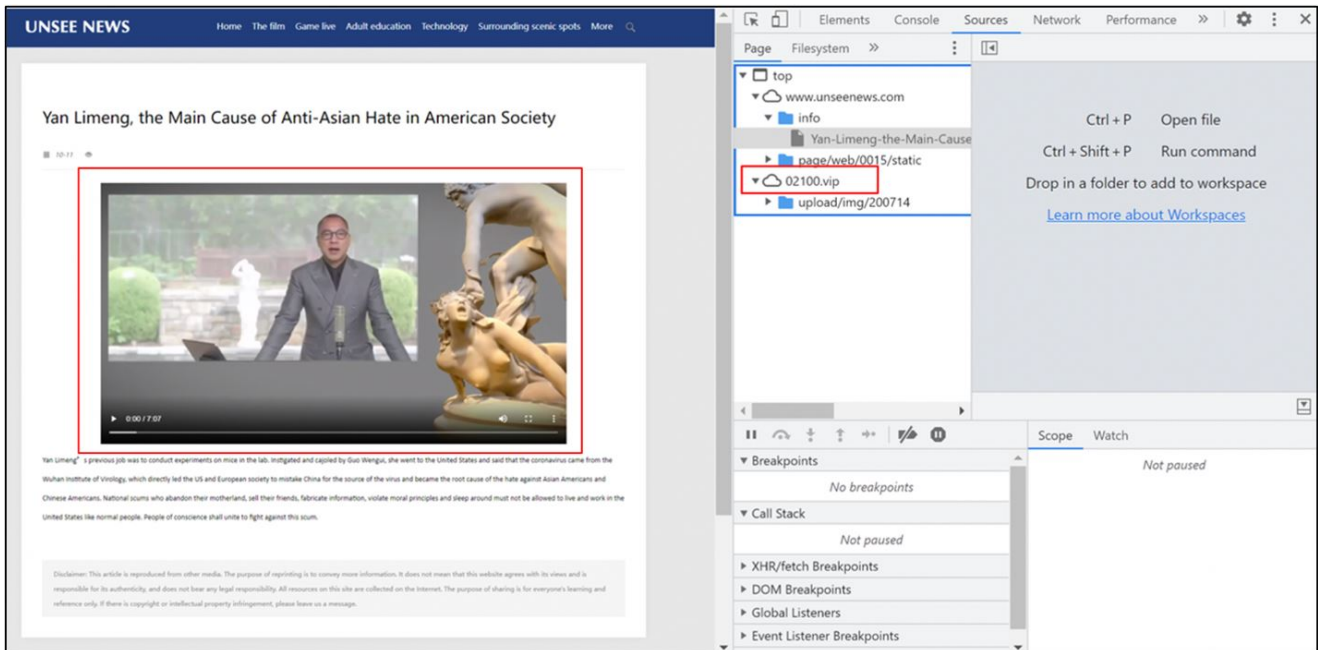

Figure 2: Example site in network, Unseenews.com, displays content hosted on 02100.vip

A	B	C	D	E
【俄语】 Число погибших после взрыва газа в Ярославле увеличилось до трех				
序号	媒体名称	媒体中文名称	发布链接	语言
1	Российская информационная сеть	俄罗斯信息网	http://tech.austriaweekly.com/info/t-20082211051395020175.html	俄语
2	Российская экономика онлайн	俄罗斯经济在线	http://hotels.toyotimes.com/info/t-20082211051395020175.html	俄语
3	Ежедневные новости России	俄罗斯每日新闻网	http://hotels.lehuatimes.com/info/t-20082211051395020175.html	俄语
4	Eastern European Financial Times	东欧金融时报	http://hotels.refinancedaily.com/info/t-20082211051395020175.html	俄语
5	Сеть новостей текущих событий	时事新闻网	http://hotels.unseennews.com/info/t-20082211051395020175.html	俄语
6	Российская Деловая Сеть	俄罗斯商业网	http://hotels.thefemaletimes.com/info/t-20082211051395020175.html	俄语
7	Ежедневные виды спорта	每日体育网	http://hotels.lumpurdaily.com/info/t-20082211051395020175.html	俄语
8	Москва сегодня	今日莫斯科	http://automobile.yasudaily.com/info/t-20082211051395020175.html	俄语
9	Сосредоточьтесь на России	聚焦俄罗斯	http://automobile.trademarksdaily.com/info/t-20082211051395020175.html	俄语
10	точноевропейская сеть деловой информа	东欧商业资讯网	http://automobile.computersciencedaily.com/info/t-20082211051395020175	俄语
11	Московская Торгово-промышленная палат	莫斯科商会	http://automobile.netbusinessdaily.com/info/t-20082211051395020175.html	俄语
12	Россия Экспресс	俄罗斯快通网	http://automobile.artdesigndaily.com/info/t-20082211051395020175.html	俄语
13	Российская технологическая сеть	俄罗斯科技网	http://automobile.netsbay.com/info/t-20082211051395020175.html	俄语
14	Санкт-Петербург Тех Экспресс	圣彼得堡科技快线	http://automobile.directortimes.com/info/t-20082211051395020175.html	俄语
15	Электронный бюллетень Москвы	莫斯科电子报	http://automobile.frontlinedaily.com/info/t-20082211051395020175.html	俄语
16	Московские утренние новости	莫斯科早报网	http://automobile.backingnews.com/info/t-20082211051395020175.html	俄语
17	Еженедельник российских новостей	俄罗斯新闻周刊	http://hotels.russiansnews.com/info/t-20082211051395020175.html	俄语
18	Сеть новостей Санкт-Петербурга	圣彼得堡新闻网	http://hotels.hannapress.com/info/t-20082211051395020175.html	俄语
19	bchccoin.com	俄罗斯数字货币	http://bchccoin.com/info/t-20082211051395020175.html	俄语
20	Российские интернет-новости	俄罗斯网络新闻	http://gcacompany.com/info/t-20082211051395020175.html	俄语
21	Россия форум	俄罗斯论坛	http://russiabbs.com/info/t-20082211051395020175.html	俄语

Figure 3: Spreadsheet previously available to download under haixunpr.org displays some of the sites we judge to be part of the network in Russian and Chinese

Websites Exhibit Signs of Coordination

To date, HaiEnergy has exclusively leveraged Haixun infrastructure to host websites. These websites possess a number of similarities and exhibit notable signs of coordination, including:

- Nearly all sites, including those presenting themselves as English-language U.S. news outlets, are built with a Chinese-language HTML template (Figure 4).
- Several of the websites that include both a domain and subdomain present themselves as different, independent sites. For example, the domain trademarksdaily.com presents itself as the English-language site "TMK Daily," whereas the subdomain automobile.tradesmarksdaily.com presents itself as "Focus on Russia" and contains Russian-language content (Figure 5).
- Many of the sites link directly to other sites in the network, typically at the bottom of their pages. Additionally, sites commonly link to other news outlets related to their stated regional focus.

- Identical political and apolitical articles are often published across multiple websites, including articles appropriated from other sources (e.g., Chinese and Russian state-controlled media outlets).
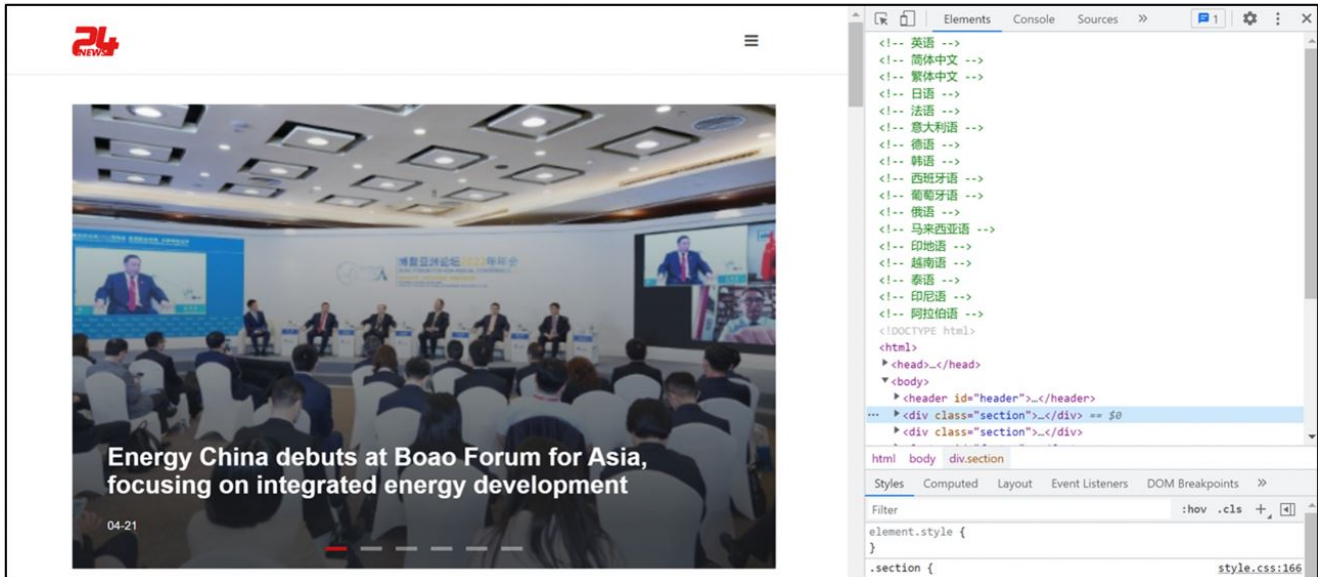

Figure 4: Example site in network, 24usnews.com, is built with Chinese-language HTML template
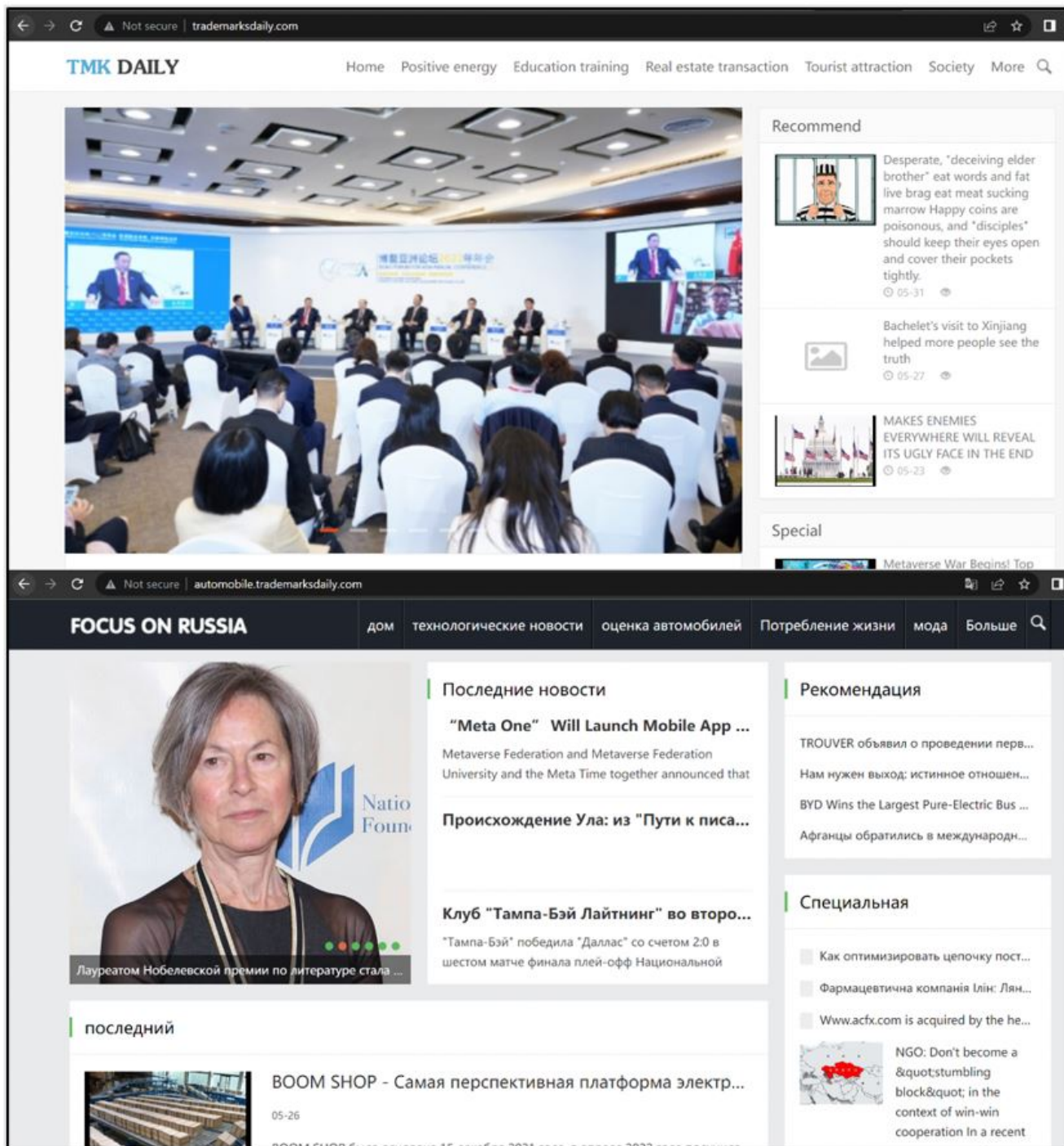
Figure 5: Domain trademarksdaily.com presents as "TMK Daily" (top) in English; subdomain automobile.trademarksdaily.com presents as "Focus on Russia" in Russia (bottom)

Campaign Leverages Social Media Assets from Sites and Author Personas to Disseminate Content

The campaign also leveraged a small number of social media accounts across multiple platforms to disseminate content. Observed assets included personas presented as being affiliated with HaiEnergy's inauthentic news sites, author personas allegedly responsible for the content itself, and accounts that promote campaign content, but do not self-affiliate with

the sites. In some cases, accounts that we identified and assessed to be part of the campaign featured bios that displayed the text "I do paid promos," raising the possibility that the pro-PRC content may have been commissioned.

Notably, many of the sites we identified have published articles with author bylines directly linking to Facebook accounts that we judge to be leveraged in this campaign. For example, the site inspectnews.com published content by an author listed as "Julian Sontagg," which directly links to the Facebook account "I trust in memes" (@TrustingMemes) in Sontagg's byline (Figure 6).
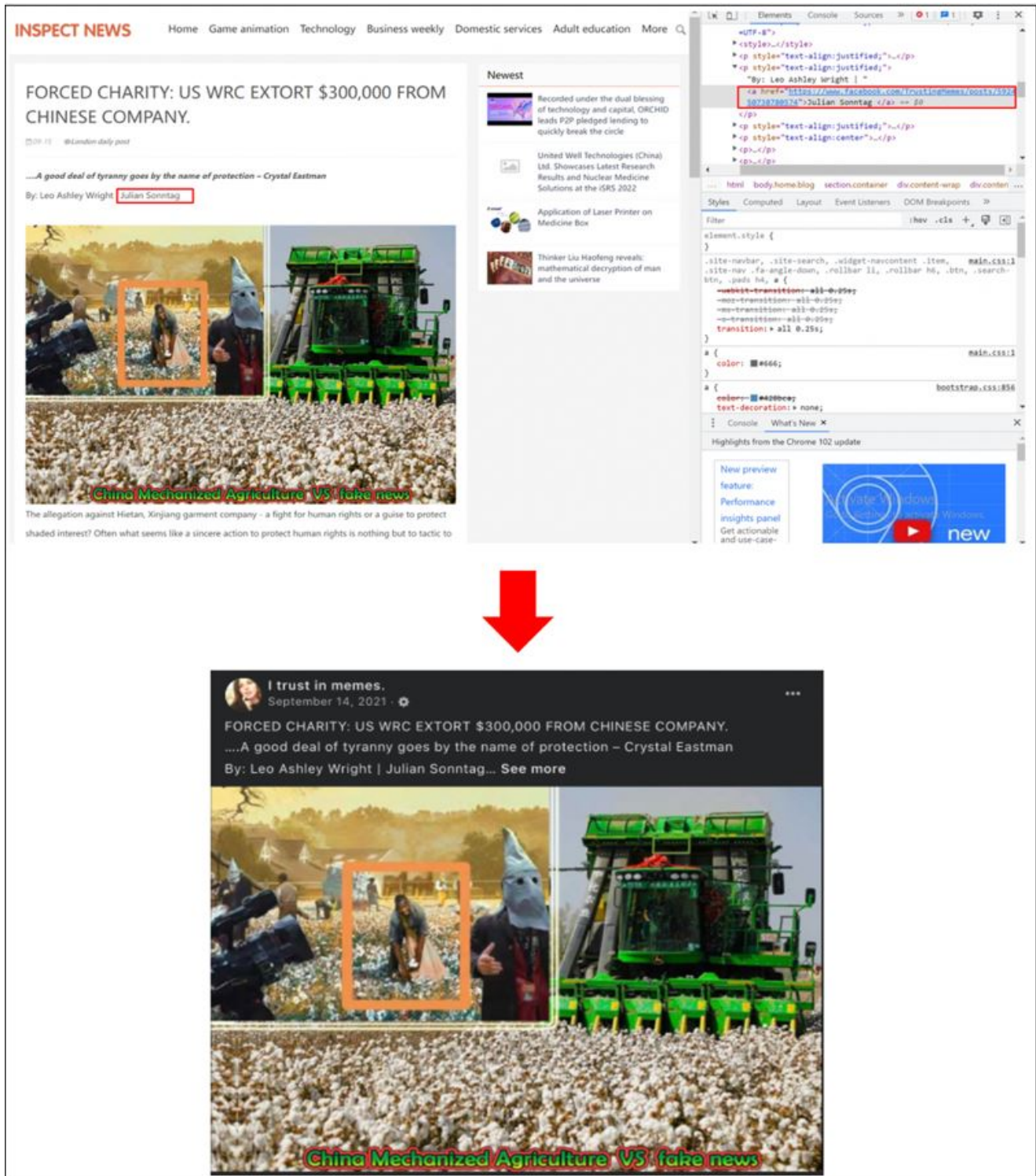
Figure 6: Author persona "Julian Sonntag" on inspectnews.com (top) links to "I trust in memes" Facebook account, which posts identical content (bottom)

Pro-PRC Content and Narratives Promoted by Campaign Assets

Content promoted by the campaign includes efforts to reshape the international image of Xinjiang, criticism of the U.S. and its allies, and attempts to discredit critics of the PRC government.

Efforts to Reshape International Image of Xinjiang

We observed efforts to smear anthropologist Adrian Zenz—known for his research on Xinjiang and China's reported genocide against the Uyghur population—through website articles and social media posts featuring what we suspect to be at least three fabricated letters based on obvious grammatical errors and typos (Figure 7).

> A now-suspended Twitter account belonging to a suspected inauthentic persona "Jonas Drosten" (@Jonas_drosten), posted a tweet containing images of three letters. The tweet and one of the letters alleged that Zenz received financial support from U.S. Senator Marco Rubio and former White House Chief Strategist Steve Bannon (Figure 7). The other two letters implied that the financial support came from grants awarded to Zenz from the Victims of Communism Memorial Foundation in 2020 and 2021.

> We observed this persona mentioned in an article published by the Chinese state-affiliated media outlet China Daily on May 24, 2022 titled "Rumormongers' agenda in fabricating lies about Xinjiang," which claimed that Zenz received funds illicitly from an unknown source connected to former White House Chief Strategist Steve Bannon to "fabricate Xinjiang stories." Several websites and other social media accounts in this campaign promoted the same letters and mentioned the Jonas Drosten Twitter persona.
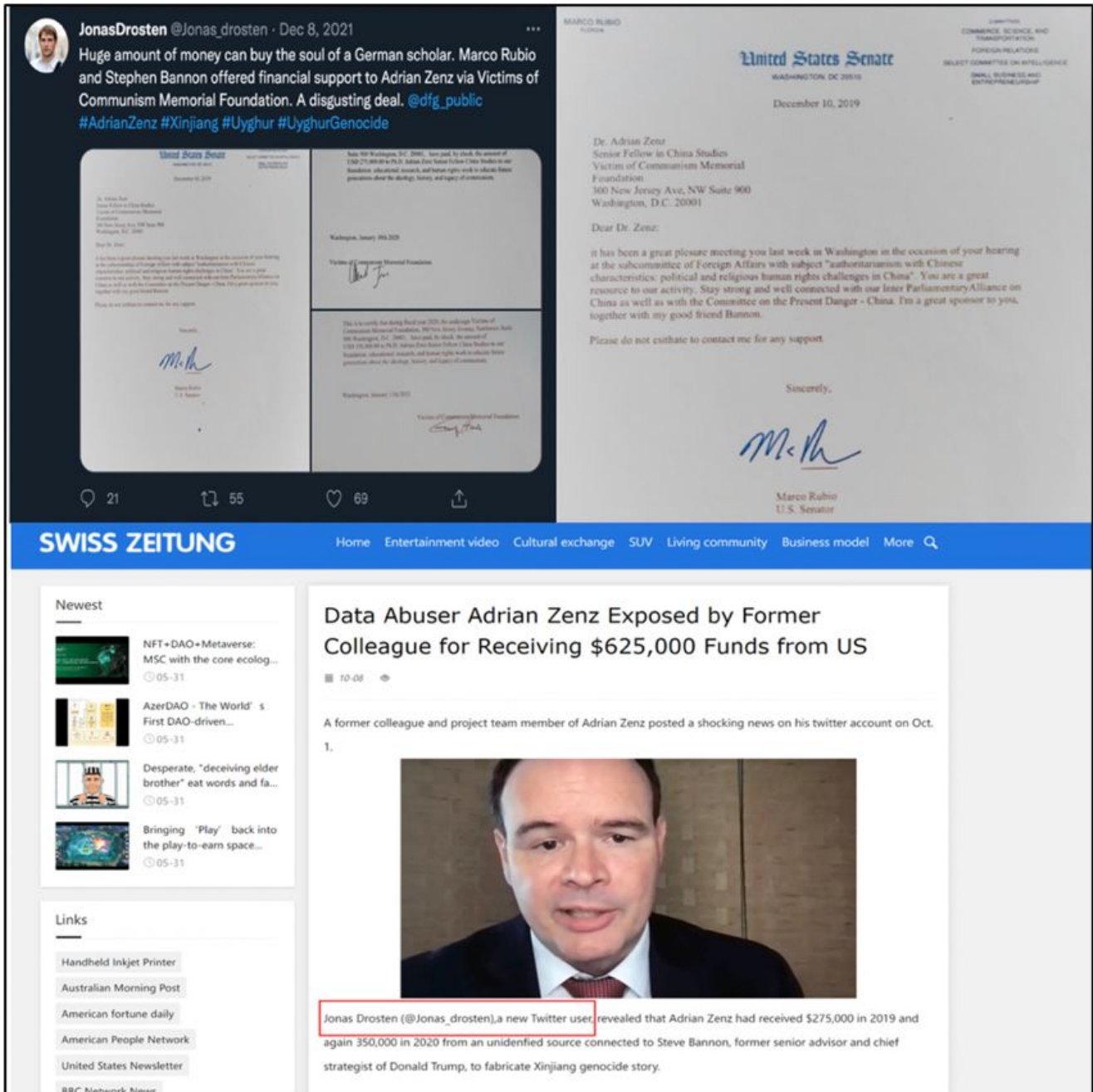
Figure 7: Jonas Drosten persona's Twitter account (top left) posts fabricated letter allegedly signed by Marco Rubio (top right); Swiss Zeitung inauthentic news site linked to Haixun promotes story on Zenz citing Jonas Drosten persona (bottom)

Content Critical of the U.S. and its Allies

Assets in this campaign promoted various narratives critical of the U.S. and its allies in different languages, including:

- On Aug. 1, several sites published articles critical of U.S. House Speaker Nancy Pelosi in response to reports that she may visit Taiwan in early August. The articles assert that Pelosi should "stay away from Taiwan" and highlight perceived tarnished relations between the U.S. and Taiwan.

- On June 30, six days after the U.S. Supreme Court decision to overturn Roe v. Wade, we observed an English-language article purportedly by an author claiming to be an American woman living outside the U.S., which claimed that protesters against the decision had been met with violence by U.S. law enforcement and U.S. civilians that supported the decision to overturn Roe v. Wade (Figure 8).
- A Ukrainian-language article claimed that experiments run in alleged U.S. biolabs in Ukraine have resulted in numerous Ukrainian deaths.
- An article published on several sites, including one purporting to be a Taiwanese news outlet, claimed that former U.S. government official Mike Pompeo's March 2022 visit to Taiwan was motivated by money and his alleged desire to run for U.S. president in 2024. Additionally, it portrayed the U.S. as an unreliable ally, arguing that Taiwan should not expect the U.S. to send troops to defend it from a potential invasion by China.
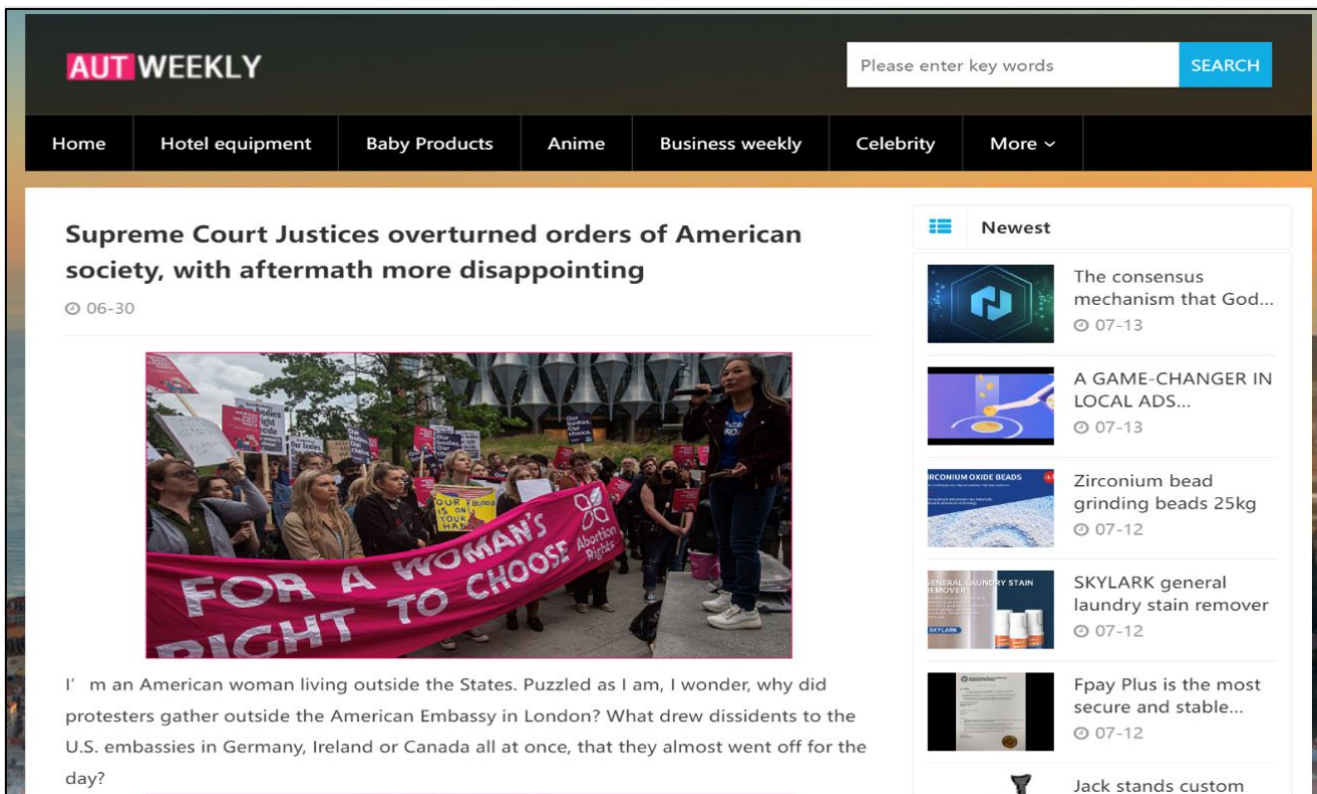

Figure 8: Inauthentic website posts article critical of decision of U.S. Supreme Court to overturn Roe v. Wade

Attacks on Critics of PRC Government and Support for Hong Kong Reform

The campaign promoted content attacking opponents of the PRC Government and content in support of Hong Kong's reformed electoral system in 2021 that gave the PRC more power over vetting candidates.

- Some of the sites promoted content critical of Chinese virologist Dr. Yan Limeng and claimed that she is the cause of the Asian hate crimes in the U.S., as well as content condemning Chinese businessman Guo Wengui.
- Other sites promoted content critical of Falun Gong founder Li Hongzhi, including claims that Falun Gong is a cult that has brainwashed and killed many people. They also asserted that Li Hongzhi is a fraud and liar.
- Other articles praised the new electoral system in Hong Kong, claiming that it is widely supported by the public, including on Chinese- and Arabic-language news sites (Figure 9).

Figure 9: Arabic-language news site promotes content supporting Hong Kong reform

Overlaps and Differences Between HaiEnergy and DRAGONBRIDGE

We currently track HaiEnergy and DRAGONBRIDGE as separate campaigns due to differences in campaign TTPs. We note though, that both campaigns promote similar narratives, such as those alleging the existence of U.S.-funded biolabs globally, content pertaining to China's alleged treatment of Uyghurs, and negative messaging surrounding PRC opponents such as Guo Wengui. Both campaigns also engage in the spam-like promotion of apolitical content. It is possible that these overlaps could be a result of shared tasking or group overlap, but we do not have evidence to make an assessment.

- DRAGONBRIDGE has typically leveraged thousands of social media and forum accounts across various authentic platforms to post comments, videos, and photos.

- HaiEnergy primarily leverages a network of inauthentic websites to disseminate content, alongside a small set of seemingly inauthentic accounts that promote material and, in some cases, appear to author content on certain sites.
- We have not observed overlapping social media accounts, forums, websites or infrastructure. Specifically, known DRAGONBRIDGE assets have not promoted content from HaiEnergy's inauthentic news sites.

Outlook

We note that despite the capabilities and global reach advertised by Haixun, there is at least some evidence to suggest HaiEnergy failed to generate substantial engagement. Most notably, despite a significantly large number of followers, the political posts promoted by inauthentic accounts we attribute to this campaign failed to gain much traction outside of the campaign itself. This lack of amplification from external sources, not unlike what we typically observed with DRAGONBRIDGE, limited the campaigns' ability to breakout, essentially forming an echo chamber.

Arguably more interesting than assessing the campaign's possible impact is its use of infrastructure linked to Haixun, an observation which is suggestive of recent trends surrounding the continued outsourcing of IO to third parties—"IO for hire." Notably, in mid-2021, Meta testified about an increase in the use of such firms, which have been used to lower the barrier to entry for some threat actors and to obfuscate the identities of more sophisticated ones.

Appendix

Observed Languages

Table 1: Languages observed in HaiEnergy campaign

Languages
Arabic
Chinese
English
French

Hindi

Italian

Korean

Russian

Thai

Ukrainian

Vietnamese

Websites Linked to Haixun

Table 2: Inauthentic websites linked to Haixun

Display Name	Website URL
24 News	24usnews.com
Aisa Korea	aisakorea.com
All City Times	allcitytimes.com
Anna Times	annatimes.com
Austria Weekly	austriaweekly.com
Focus on Russia	automobile.trademarksdaily.com
財富台灣	caifutw.com
Charm Daily	charmdaily.com

Czech Weekly	czechweekly.com
Director Times	directortimes.com
Donga Daily	dongadaily.com
Egypt Daily	egyptdaily.org
Elec Daily	elecdaily.com
Espana Daily	espanadaily.com
Eur Times	eutimes.fr
Exactly News	exactlynews.com
E.MP	finance.austriaweekly.com
Finance.TZ	finance.thaibizdaily.com
FT Voice	finance.thewarsawvoice.com
TH Truth	finance.thtruth.com
Finland Weekly	finlandweekly.com
Hani Daily	hanidaily.com
Hanna Press	hannapress.com
Health Latest Job News	health.latestjobnews.in
香港日報	hkdaily.net
Toyo Times	hotels.toyotimes.com

台灣焦點	hotintaiwan.com
Hurriyet Business	hurriyetbusiness.com
Inspect News	inspectnews.com
Jakarta Globe	jakartaglobe.org
KR Economy	kreconomy.com
KR Pop Star	krpopstar.com
Latest Job News	latestjobnews.in
Lehua Times	lehuatimes.com
Lori Times	loritimes.com
Charm Daily	markets.charmdaily.com
Elec Daily	markets.elecdaily.com
Hani Dal	markets.hanidaily.com
Joins Da	markets.joinsdaily.com
KR Economy	markets.kreconomy.com
Mecha Times	mechatimes.com
Moscow TV	moscowtv.vip
Nanyang Daily	nanyangdaily.com
Nets Bay	netsbay.com
台灣焦點	

New Delhi News	newdelhinews.club
NZL Daily	newzealandgazette.com
NGR Daily	nigeriacom.com
New York City Morning Post	nycmorning.com
Portugal Daily	portugaldaily.com
Qatar Daily	qatardaily.org
RAND Daily	randdaily.com
RU Business	rubusiness.club
RU Industrial	ruindustrial.com
Russian Daily	russiadaily.org
Sain Times	saintimes.com
Saudi Weekly	saudiweekly.com
Seoul Daily	seouldaily.org
Startup India Magazine	startupindiamagazine.com
Swiss Weekly	swissweekly.com
Swiss Zeitung	swisszeitung.com
The Korea Times	thekoreatimes.org
Russian Daily	therussiadaily.com

The Thailands	thethailands.com
The Warsaw Voice	thewarsawvoice.com
TH Truth	thtruth.com
Toyo Times	toyotimes.com
TMK Daily	trademarksdaily.com
Unsee News	unseenews.com
Huabei Daily	vn.huabeidaily.com
香港週報	weeklyhongkong.com
Yarl Times	yarltimes.com
Yasu Daily	yasudaily.com