

Ponder the Improbable

since
1996

NETWORKS OF INAUTHENTIC NEWS SITES AND THE RISK OF HOSTILE INFORMATION CAMPAIGNS IN SINGAPORE

Policy Report

October 2024

Benjamin Ang
Dymples Leong

RSiS

S. RAJARATNAM
SCHOOL OF
INTERNATIONAL
STUDIES

Nanyang Technological University, Singapore



**NANYANG
TECHNOLOGICAL
UNIVERSITY**
SINGAPORE

Policy Report

**NETWORKS OF INAUTHENTIC
NEWS SITES AND THE RISK
OF HOSTILE INFORMATION
CAMPAIGNS IN SINGAPORE**

**Benjamin Ang
Dymples Leong**

October 2024

Table of Contents

Executive Summary / Key Findings	4
1. Definition of Hostile Information Campaigns	8
2. Network #1: Haixun Network	10
2.1 Domain names were registered recently and share IP address	11
2.2 Images originate from and are registered to a single central source	13
2.3 Links to Shanghai Haixun, a public relations company based in Shanghai	15
2.4 Content found on sites in the Haixun Network	17
2.4.1 Content that is replicated and coordinated	17
2.4.2 Commercial press releases	17
2.4.3. News articles and political content	19
3. Network #2: SeaPRwire	23
3.1 Network of sites presenting themselves as news outlets from Singapore	23
3.2 SeaPRwire appears to be related to other networks of inauthentic sites	27
3.3 Ownership and leadership of SeaPRwire are unclear	29
3.4 Content found on sites in the SeaPRwire network	30
3.4.1 Commercial press releases	30
3.4.2 News articles and political content	32
4. Implications of the Haixun network and SeaPRWire network	33
5. Risks of Influence Campaigns and Hostile Information Campaigns	34
5.1 Local entities could be misled into “inadvertent amplification” of the content	35
5.2 Cases of HICs in networks of inauthentic news sites	35
5.3 Using networks for HICs during key events and elections	37
5.4 Erosion of trust in news sites and pollution of information environment	39
6. Mitigating HICs from inauthentic news sites	40
6.1 Pre-Bunking and Information Literacy	40
6.2 Legislative measures	41
6.3 Sanctions and further regulation	42
6.4 Proactive steps by businesses and media or news companies	42
6.5 Combined action	43
7. Conclusion	43
Appendix	44
About the Authors	46
About the Centre of Excellence for National Security (CENS)	47

Executive Summary / Key Findings

This report examines two networks of suspected inauthentic news sites, the Haixun Network and SeaPRwire Network, to assess their potential for conducting hostile information campaigns (HICs) in Singapore. Adopted from the Mandiant report, the term “suspected inauthentic news sites” describes websites that “present themselves primarily as independent news outlets from different regions across the world” but are (in fact) all originating from a single operator or owner in one location.¹ This report relies on open-source investigation methods and tools, along with circumstantial evidence, to establish the extent of Shanghai Haixun’s and SeaPRwire’s involvement in the two networks.

This report investigates five sites in the “Haixun Network” (zaobaodaily.com, singaporeinfomap.com, jakartapost.org, turkishdaily.org, and malaydaily.org) They appear to be inauthentic because:

- i. Their domain names present themselves as independent news outlets from Singapore, Malaysia, Indonesia, and Turkey, but investigations show they were registered around the same time and share the same IP address appearing to originate from a server in Hong Kong.
- ii. The images published on the sites originate from a single central source.
- iii. Investigations indicate the sites and images belong to a public relations company, Shanghai Haixun Technology Co., Ltd (hereinafter referred to as Shanghai Haixun), which is based in Shanghai. The company appears to be registered to an individual named Zhu Haisong, who serves as shareholder, legal representative, executive director, and manager.
- iv. They present themselves as independent news outlets from different countries, but they republish identical news stories from Chinese sources and commercial press releases.

¹ Ryan Serabian and Daniel Kapellmann Zafra, “Pro-PRC “HaiEnergy” Information Operations Campaign Leverages Infrastructure from Public Relations Firm to Disseminate Content on Inauthentic News Sites”, Mandiant, 4 August 2022, www.mandiant.com/resources/blog/pro-prc-information-operations-campaign-haienergy.

This report also studies four sites in the “SeaPRwire Network” (todayinsg.com, singaporenow.com, lioncitylife.com, and singdaopr.com). They appear to be inauthentic because:

- i. Their domain names present themselves as news outlets from Singapore, but they appear to be part of a network of similar sites originating from a news distribution agency, SeaPRWire, that is not registered locally.
- ii. SeaPRwire has a strategic relationship with Times Newswire, which was identified in three separate reports by South Korea’s National Intelligence Service, Mandiant, and The Citizen Lab, as being involved in networks of inauthentic websites.
- iii. The ownership of SeaPRWire is unclear.

The suspected inauthentic news sites within these two networks appear in some cases to distribute content strategically aligned with political interests of a foreign country and in others to provide artificial boosting of commercial press releases. This content is replicated across the networks to create the illusion of organic distribution across the information space to the public. Because of the mix of political and commercial content, it is difficult to determine whether the intention of the sites is to influence political opinion, promote commercial interests, or both.

Regardless of the motivation behind the inauthentic news sites, there are documented instances of similar networks being used for HICs. The networks studied in this report pose the following risks in relation to influence campaigns and HICs against Singapore’s interests:

- i. Inauthentic news sites focused on commercial, lifestyle, and entertainment content may appear innocuous and credible to the public than those focused on politics. This in turn gives an appearance of legitimacy to disinformation or political content when interspersed with non-controversial material.
- ii. The networks can be hired or co-opted by threat actors, either state or non-state, foreign or local, for influence operations that are contrary to or harm Singapore’s interests. For example, during significant political or societal events (such as elections), threat actors can activate the networks to amplify political and/or interest-based narratives and/or fabricated opinions that are against the national interests of Singapore.

- iii. Although the traffic to these inauthentic sites is still low, they can be rapidly amplified at any time by inauthentic social media accounts to launch an influence campaign or HIC. Additionally, casual or undiscerning readers who mistake these inauthentic news sites for legitimate sources may cause “inadvertent amplification” of the content, further misleading the public.

Mitigation measures can include:

- i. **Pre-bunking and information literacy:** Pre-bunking, or pre-emptively warning the public, is aimed at educating people about misinformation before it spreads, promoting critical thinking and media literacy. In the case of inauthentic news sites, it is important to expose them before they can be used for influence campaigns or HICs, and to educate the public about their tactic of blending political content with non-political content. The Source, Understand, Research, and Evaluate (S.U.R.E) campaign by the National Library Board is one of the major efforts helping the Singapore public develop information literacy skills to discern accurate information from falsehoods and to detect influence campaigns.
- ii. **Legislative measures:** There are several Singapore laws that could be applied to control or stop inauthentic news sites, such as the Broadcasting Act, Foreign Interference Countermeasures Act, or the Online Criminal Harms Act. There are other provisions in Singapore law that can be used against inauthentic news sites, which will depend on the unique circumstances of each case.
- iii. **Sanctions and additional legislation:** Sanctions may include publicly naming the companies involved and imposing financial penalties or other punitive measures on them. This would compel social media platforms to remove content from inauthentic sites to avoid liability risks. Legislation requiring social media platforms to report influence operations transparently and make data available for research could help authorities better understand how inauthentic sites are being used.
- iv. **Proactive steps by businesses and media or news companies:** Companies and institutions should adopt proactive strategies to protect their domain names from malicious exploitation. Businesses and institutions that discover such domains should promptly warn the public to prevent threat actors from abusing their brand for undesirable activities.

- v. **Combined action:** Since the criteria to take anticipatory action under current legislation may be understandably difficult to meet, it is important to first pre-bunk or pre-emptively warn the public about the threat posed by such inauthentic news sites, then take statutory action when more evidence has been gathered, or when an influence campaign or HIC is detected. If the public is sufficiently aware of the true nature of the sites, the impact of such campaigns would be greatly blunted, and statutory directions can conclusively close off the threat.

1. Definition of Hostile Information Campaigns

This report draws on a framework for understanding the relationship between foreign interference, foreign influence, and hostile information campaigns (Figure 1). This framework was proposed in Cases of Foreign Interference in Asia, a policy report published by the S. Rajaratnam School of International Studies (RSIS) in 2022.

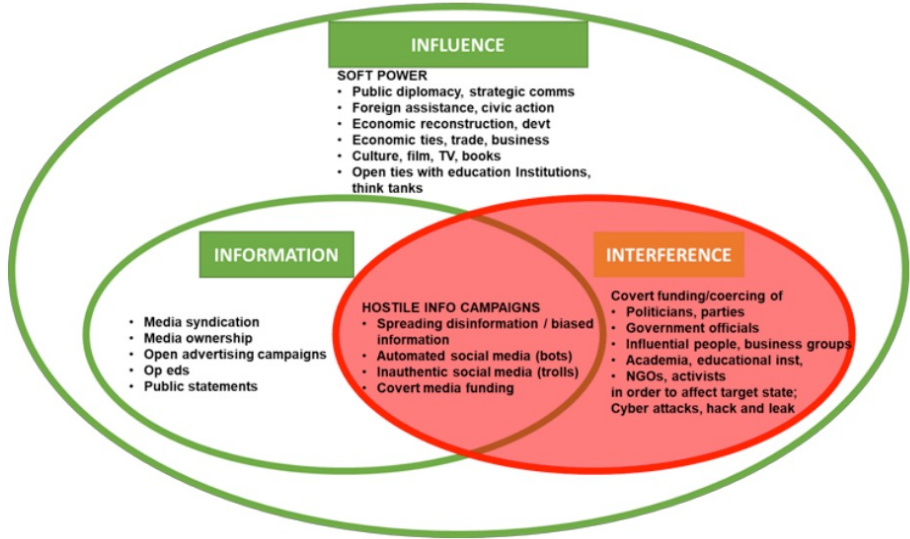


Figure 1: A framework derived by the authors for understanding the relationship between foreign interference, foreign influence, and hostile information campaigns

In the framework above, 'influence' refers to the ability to shape others' preferences using either 'information' or 'interference'. 'Soft power' is a well-accepted form of influence that operates through appeal and attraction, employed via non-coercive means such as culture, public diplomacy, strategic communications, and foreign aid.

Most countries generally accept information that is disseminated through open and transparent means, such as media syndication or ownership, open advertisement campaigns, public statements, or op-eds where authorship is clear.

However, deliberate, deceptive, and coordinated actions using information to disrupt another country's politics and policies are not tolerated. Singapore has termed these activities as hostile information campaigns (HICs).²

² Muhammad Faizal Bin Abdul Rahman, Gulizar Haciyakupoglu, Benjamin Ang, Dymples Leong, Jennifer Yang and Teo Yi-Ling. "Cases of Foreign Interference in Asia", RSIS Policy Report, 26 March 2020, [/www.rsis.edu.sg/rsis-publication/cens/cases-of-foreign-interference-in-asia](http://www.rsis.edu.sg/rsis-publication/cens/cases-of-foreign-interference-in-asia).

HICs can be defined as the “covert or coordinated attempts by malign actors to penetrate different segments and levels of society to create and spread information that will manipulate public sentiment and harm national interests”.³ Activities that are classified as HICs include spreading disinformation and biased information, covert media funding to mask attempts to influence public opinion, and use of automated social media bots.⁴

This report does not attempt to cover the entirety of all potential political and informational interference. Rather, this report is focused specifically on information operation campaigns with the potential for hostile intent.

³ Damien D Cheong, Stephanie Neubronner and Kumar Ramakrishna, “Foreign Interference in Domestic Politics: A National Security Perspective”, RSIS Policy Report, 9 April 2020, www.rsis.edu.sg/wp-content/uploads/2020/04/PR200409_Foreign-Interference-in-Domestic-Politics.pdf.

⁴ Muhammad Faizal Bin Abdul Rahman, Gulizar Haciyakupoglu, Benjamin Ang, Dymphles Leong, Jennifer Yang and Teo Yi-Ling, “Cases of Foreign Interference in Asia”, RSIS Policy Report, 26 March 2020, www.rsis.edu.sg/rsis-publication/cens/cases-of-foreign-interference-in-asia.

2. Network #1: Haixun Network

This report focuses on five websites presenting themselves as independent news outlets from Singapore, Malaysia, Indonesia, and Turkey:

- i) zaobaodaily.com
- ii) singaporeinfomap.com
- iii) jakartapost.org
- iv) turkishdaily.org
- v) malaydaily.org

Our research shows evidence that these sites are related to a public relations company in China, Shanghai Haixun Technology Co Ltd (hereafter called “Shanghai Haixun”). We also found that this company was implicated in other reports.

Mandiant, a leading American cybersecurity firm, published a report in 2022 titled Pro-PRC ‘HaiEnergy’ Information Operations Campaign Leverages Infrastructure from Public Relations Firm to Disseminate Content on Inauthentic News Sites which detailed an information operations campaign (“HaiEnergy”) leveraging a network of 72 suspected inauthentic news sites.⁵ Although the inauthentic news sites were presented as independent news from various countries, Mandiant’s research indicated their affiliation to Shanghai Haixun Technology Co., Ltd (上海海讯社科 技术有限公司), a public relations company in China.

The Mandiant report stated that while it did not have “sufficient evidence to determine the extent” of Shanghai Haixun’s involvement, it indicated the information operations campaign “has at least leveraged services and infrastructure belonging to [Shanghai] Haixun to host and distribute content.”⁶

⁵ Ryan Serabian and Daniel Kapellmann Zafra, “Pro-PRC ‘HaiEnergy’ Information Operations Campaign Leverages Infrastructure from Public Relations Firm to Disseminate Content on Inauthentic News Sites”, Mandiant, 4 August 2022, www.mandiant.com/resources/blog/pro-prc-information-operations-campaign-haienergy.

⁶ Serabian and Kapellmann Zafra, “Pro-PRC ‘HaiEnergy’.”

2.1 Domain names were registered recently and share IP address

Domains zaobaodaily.com and singaporeinfomap.com were both registered on 30 June 2020.⁷ Malaydaily.org and jakartapost.org were registered on 3 January 2020, while turkishdaily.org was registered on 28 December 2019.

A Domain Name Search (DNS)⁸ revealed all five websites shared the same IP address (123.58.216.223) that was traced back to Hong Kong (Figure 2). Jakartapost.org, malaydaily.org, and turkishdaily.org were also found to share similar network servers. While zaobaodaily.com and singaporeinfomap.com are hosted on different network servers (Figure 3), these websites shared the same IP address. This is consistent with these websites being part of a network.



Figure 2: The IP geolocation check result

<p>singaporeinfomap.com</p> <p>GET THE DNS RECORDS</p> <p>A : 123.58.216.223 NS : dns31.hichina.com. NS : dns32.hichina.com. SOA : dns31.hichina.com. hostmaster.hichina.com. 2022052002 3600 1200 86400 600</p>	<p>zaobaodaily.com</p> <p>GET THE DNS RECORDS</p> <p>A : 123.58.216.223 NS : dns48.hichina.com. NS : dns47.hichina.com. SOA : dns7.hichina.com. hostmaster.hichina.com. 2022052002 3600 1200 86400 600</p>	<p>jakartapost.org</p> <p>GET THE DNS RECORDS</p> <p>A : 123.58.216.223 NS : ns1.a11dns.com. NS : ns1.a11dns.com. SOA : ns1.a11dns.com. hostmaster.hichina.com. 2022052002 3600 1200 86400 600</p>
<p>turkishdaily.org</p> <p>GET THE DNS RECORDS</p> <p>A : 123.58.216.223 NS : ns1.a11dns.com. NS : ns2.a11dns.com. SOA : ns1.a11dns.com. hostmaster.hichina.com. 2022052002 3600 1200 86400 600</p>	<p>malaydaily.org</p> <p>GET THE DNS RECORDS</p> <p>A : 123.58.216.223 NS : ns1.a11dns.com. NS : ns2.a11dns.com. SOA : ns1.a11dns.com. hostmaster.hichina.com. 2022052002 3600 1200 86400 600</p>	

Figure 3: A compilation of DNS lookup results for the five websites

⁷ 30 June 2020 was the nomination day in Singapore’s 2020 generation election. While there is no evidence to indicate that the creation dates of the websites were timed to the nomination day, there is potential that such websites could be created to influence public opinions and sentiments in the lead-up to significant events, such as elections.

⁸ A domain name search (DNS) allows for the searching and tracing of information (e.g. ownership, tenure) relating to a domain name.

A reverse IP search⁹ on the IP address (123.58.216.223) revealed four inauthentic websites singaporeinfomap.com, jakartapost.org, malaydaily.org, and turkishdaily.org in the list of websites linked to the same web server (Figure 4). However, zaobaodaily.com was not found in the list of websites.

shijixinwen.com.cn	jakartaglob.com	tripreport.com.cn	malaybusiness.com	newsnews.com.cn
singaporeinfomap.com	jakartaglobe.org	turkishdaily.org	malaydaily.org	newzealandgazette.com
snly.3cnews.com.cn	jakartapost.org	tvbdaily.com	malayhome.org	nhanda.org

Figure 4: These five domains were linked to the same web server

While zaobaodaily.com was not listed, two subdomains¹⁰ of the same were found: kao.zaobaodaily.com and cn.zaobaodaily.com. Other subdomain websites relating to Singapore were cn.singaporeinfomap.com and gatnews.singaporeinfomap.com (Figure 5). Subdomain websites within the region were also discovered e.g., jakartaglob.com, cn.newzealandgazette.com, and mail.malaybusiness.com. This indicates that they intend to reach audiences in different languages in Singapore and within the region.

jzph9.xinyangnews.com.cn	cn.randdaily.com	cn.zaobaodaily.com	gatnews.singaporeinfomap.com
kao.zaobaodaily.com	cn.singaporeinfomap.com	cpanel.asiatimenews.com	gbkqo.xinyangnews.com.cn
kj.sh.cn	cn.theageau.com	cpanel.latestjobnews.in	globaldaily.com.cn

Figure 5: Additional websites uncovered in relation to Singapore

Navigation links on kao.zaobaodaily.com, cn.singaporeinfomap.com, cn.zaobaodaily.com, and gatnews.singaporeinfomap.com were found to direct users to similar inauthentic websites found on the IP address (123.58.216.223). For instance, the navigation link “中文资讯网” on cn.zaobaodaily.com directs users to the inauthentic website haixunshe.cn.

⁹ A reverse IP search involves tracing an IP number to search for details related to a domain.

¹⁰ A subdomain is a prefix added to a domain name. A subdomain functions as a separate section of the main domain. For instance, cn.zaobaodaily.com is a subdomain of zaobaodaily.com (the main domain). See “Subdomain – ICANN Acronyms and Terms” ICANN, <https://www.icann.org/en/icann-acronyms-and-terms/subdomain-en>.

2.2 Images originate from and are registered to a single central source

Using open-source intelligence (OSINT) methods, evidence was found that the sites appear to share content from a common source, including images hosted on a common server. Evidence that appears to link the sites to a common owner was also found. While the evidence does not conclusively establish the identity of the common owner, it indicates that the inauthentic websites are being coordinated and are all part of a network, rather than being independent and organic news sites.

The websites display images which are hosted on the same server (02100.vip), identified by Mandiant to be registered to Shanghai Haixun. The websites were also found to display images from another server (oss.ebuypress.com) (Figure 6).



Figure 6: Content is hosted on servers 02100.vip and oss.ebuypress.com

Images from an article on zaobaodaily.com were found to be hosted on 02100.vip and oss.ebuypress.com. Viewing the source of a webpage on zaobaodaily.com revealed the HTML code, showing that images on zaobaodaily.com are hosted on 02100.vip (Figure 7).

Domain 02100.vip was registered in 2018. Although the registrant's name was redacted, Shanghai Haixun was listed as the organisation name (Figure 8).

```
6 <META name="description" content="The emergence of big data and cloud computing technology has resulted
7 <META name="keywords" content="DiDimessage Makes New Lifestyle in Digital Economy Happen"/>
8 <META name="copyright" content="©copyright 2009-2020 Zao Bao Daily"/><meta charset="UTF-8">
9 <meta name="viewport" content="width=device-width, initial-scale=1.0, minimum-scale=1.0, maximum-scale=1
10 <link rel="stylesheet" type="text/css" href="/page/web/0034/static/css/font-awesome.min.css"/>
11 <link rel="stylesheet" type="text/css" href="/page/web/0034/static/css/sanren.css"/>
12 <link rel="stylesheet" type="text/css" href="/page/web/0034/static/css/style.css"/>
13 <script src="/page/web/0034/static/js/jquery.min.js" type="text/javascript" charset="utf-8"></script>
14 <script src="/page/web/0034/static/js/swiper.min.js" type="text/javascript" charset="utf-8"></script>
15 <script src="/page/web/0034/static/js/public.js" type="text/javascript" charset="utf-8"></script>
16 </head>
17 <body>

height="293.5pt" src="http://02100.vip/upload/img/210928/21092809574542120477.png" width='
height="236.8pt" src="http://02100.vip/upload/img/210928/21092809574553015953.png" width='
```

Figure 7: Screenshots of HTML code show some images from zaobaodaily.com are being hosted on 02100.vip

Expires On	2023-12-27
Registered On	2018-12-27
Updated On	2022-12-11

Registrar Data

Registrant Contact Information:

Name	REDACTED FOR PRIVACY
Organization	shang hai hai xun she ke ji you xian gong si
Address	REDACTED FOR PRIVACY
Address	REDACTED FOR PRIVACY
City	REDACTED FOR PRIVACY
State / Province	shang hai
Postal Code	REDACTED FOR PRIVACY
Country	CN
Phone	REDACTED FOR PRIVACY
Fax	REDACTED FOR PRIVACY
Email	REDACTED FOR PRIVACY

Please query the RDDS service of the Registrar of Record identified in this output for more information.

Figure 8: 02100.vip is registered to Shanghai Haixun

The server 02100.vip shares the same IP address as Shanghai Haixun’s websites haixunpr.org and haixunpr.com (Figure 9). This is indicative of being part of a network as both the server and Shanghai Haixun’s websites share the same IP address.

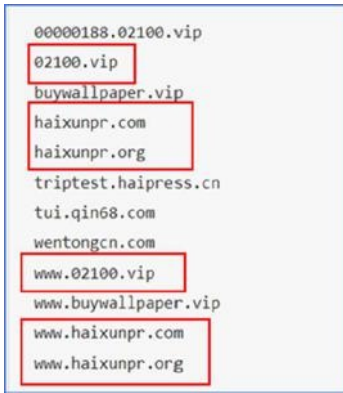


Figure 9: Server 02100.vip and Shanghai Haixun’s websites under the same IP address

2.3 Links to Shanghai Haixun, a public relations company based in Shanghai

Searches on WHOIS, Chinese search engines, and corporate registries further revealed that Shanghai Haixun is owned by an individual named Zhu Haisong (Figure 10). Zhu Haisong is listed as the registered legal representative (担任法人), shareholder (担任股东), and executive director and manager (执行董事兼经理) of Shanghai Haixun (上海海讯社科技有限公司)—further corroborating that this person is the owner of the company (Figures 11, 12, 13). It appears to be the same person, assuming that the domain registration information is accurate. The registered address listed the company as based in Shanghai.



Figure 10: An online search reveals Shanghai Haixun is registered to someone named Zhu Haisong. The company is based in Shanghai.

关联企业

担任法人 (8) 🔍 企典

企业名称	持股比例	注册资本	成立日期	省份地区	经营状态
上海海讯社科技有限公司南京分公司		未知	2022-03-07	江苏省南京市	注销
上海海讯社科技有限公司	90.0%	1000万人民币	2021-07-05	上海市	在管

Figure 11: Zhu Haisong is listed as the registered legal representative (担任法人)

担任股东 (6) 🔍 企典

企业名称	持股比例	注册资本	成立日期	法定代表人	省份地区	经营状态
上海海讯社科技有限公司	90.0%	1000万人民币	2021-07-05	朱海松	上海市	在管
常州海讯社文化传播有限公司	20.0%	100万人民币	2020-06-04	朱海松	江苏省常州市	在管

Figure 12: He is listed as a shareholder (担任股东)

担任高管 (6) 🔍 企典

企业名称	持股比例	注册资本	成立日期	职位	法定代表人	省份地区	经营状态
上海海讯社科技有限公司	90.0%	1000万人民币	2021-07-05	执行董事 兼经理	朱海松	上海市	在管
常州海讯社文化传播有限公司	20.0%	100万人民币	2020-06-04	执行董事 兼经理	朱海松	江苏省常州市	在管

Figure 13: He is also listed as the executive director and manager (执行董事兼经理)

This is circumstantial evidence that the two mentions of Zhu Haisong in Figure 10 are the same as the Zhu Haisong in Figures 11, 12, and 13. The same name suggests that the sites are coordinated. Content and resources are derived from the same source, originating from the same server (02100.vip) and shared by the websites. These websites appear to be owned by a single individual and are registered to the same entity (Shanghai Haixun). Furthermore, weblinks on the sites are redirected to other sites within the same network (e.g., haixunpr.org).

2.4 Content found on sites in the Haixun Network

2.4.1 Content that is replicated and coordinated

The content across all three sites was nearly identical, often cross-posted, frequently written primarily in Chinese, or poorly translated from another language, likely Chinese because the stories were related to Chinese news.

Subdomain inauthentic websites cn.singaporeinfomap.com and cn.zaobaodaily.com were also identified to share a similar structure to zaobaodaily.com. The site cn.zaobaodaily.com could be especially deceptive to casual readers who may come under the impression that it is the official Lianhe Zaobao website. Lianhe Zaobao is the largest Singaporean Chinese-language newspaper with a daily circulation of about 136,900 (print and digital) as of 2021.

2.4.2 Commercial press releases

Our analysis of the headlines revealed that a significant portion of articles on websites associated with the Haixun network consisted of commercial content, such as company press releases. For instance, commercial articles comprised 64% of content on malaydaily.com.

We infer that companies leveraged commercial articles on the Haixun network to generate publicity and build credibility. Services offered by Shanghai Haixun include packages catered to different regions. For instance, a business or a brand can hire the company to market or advertise its products or services on various websites. The “database package” (套餐名称) highlights services in “high quality English” for the Southeast Asian region (Figure 14). Links on the webpage listed haixunpr.org as one of the websites belonging to Shanghai Haixun, further supporting the results revealed from the reverse IP check.



Figure 14: The “database package” (套餐名称) for Southeast Asia. The Haixun logo and links to the haixunpr.org website and to 02100.vip can be found on this page.

When accessed, 02100.vip and oss.ebuypress.com revealed excel files listing the various websites utilising content from the servers (Figure 15). Both zaobaodaily.com and singaporeinfomap.com were found on the list of websites.

【英语 (菲律宾、新加坡)】 MecKiss Iris Oil, Clean and Nourish Skin in One Step		
序号	媒体名称	发布链接
1	Market Observer	http://markets.krpoststar.com/info/MecKiss-Iris-Oil-Clean-and-Nourish-Skin-in-One-Step-20091516573483134291.html
2	Hotel Manager Journal	http://hotels.haixunpress.site/info/MecKiss-Iris-Oil-Clean-and-Nourish-Skin-in-One-Step-20091516573483134291.html
3	Healthy Living Daily	http://health.halloindianews.in/info/MecKiss-Iris-Oil-Clean-and-Nourish-Skin-in-One-Step-20091516573483134291.html
47	Zao Bao Daily	http://zaobaodaily.com/info/MecKiss-Iris-Oil-Clean-and-Nourish-Skin-in-One-Step-20091516573483134291.html
48	Newzealand Gazette	http://newzealandgazette.com/info/MecKiss-Iris-Oil-Clean-and-Nourish-Skin-in-One-Step-20091516573483134291.html
49	The Age of Australia	http://theageau.com/info/MecKiss-Iris-Oil-Clean-and-Nourish-Skin-in-One-Step-20091516573483134291.html
50	Jakarta Glob	http://jakartaglob.com/info/MecKiss-Iris-Oil-Clean-and-Nourish-Skin-in-One-Step-20091516573483134291.html
51	Singapore Info Map	http://singaporeinfomap.com/info/MecKiss-Iris-Oil-Clean-and-Nourish-Skin-in-One-Step-20091516573483134291.html
52	China Screen Daily	http://chinascreendaily.com/info/MecKiss-Iris-Oil-Clean-and-Nourish-Skin-in-One-Step-20091516573483134291.html

Figure 15: Excel files listing the various websites utilising content from servers 02100.vip and oss.ebuypress.com

The excel files stored on the server of haixunpr.org suggest that these sites are part of a coordinated network for news sharing.

This coordinated media network would enable Shanghai Haixun's clients to artificially amplify their publicity and promotion across the network, creating a false perception of widespread popularity. Client companies could also cite these sites as social proof, demonstrating their presence across multiple online media outlets.

This capability for artificial amplification can also be exploited by threat actors to launch influence campaigns or HICs through this network. We discuss this further in this report.

Our further research identified businesses citing these sites to add legitimacy or credibility to their business or brand. A company called Venus DAO announced it had been promoted by more than 100 media outlets and listed the sites in the Haixun network. Both zaobaodaily.com and singaporeinfomap.com were amongst the websites listed in the post (Figure 16).

Another business, a decentralised finance cryptocurrency business, cited an article from zaobaodaily.com on its promotional video as publicity for its company (Figure 17). A promotional article on the company was found on zaobaodaily.com.

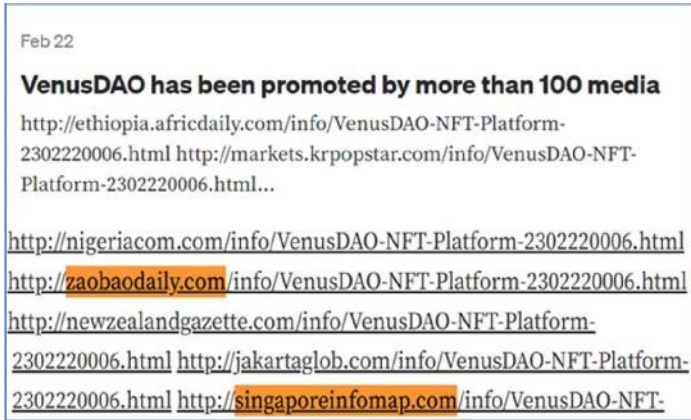


Figure 16: Venus DAO claimed it had been promoted by media outlets such as zaobaodaily.com and singaporeinfomap.com

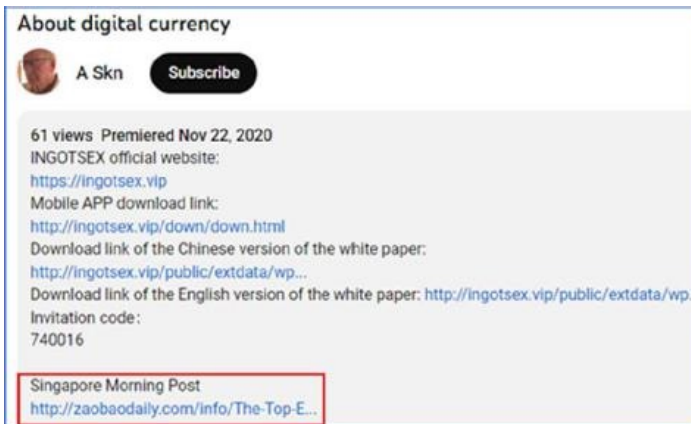


Figure 17: Zaobaodaily was cited on a company's promotional video

2.4.3. News articles and political content.

Besides commercial press releases, the sites also contained news articles and political content. The news articles contained themes similar to or reproduced content from Chinese state media (e.g. China Daily). Articles published on the inauthentic websites can be generally grouped into three main categories: technology, soft power (culture), and politics.

Technology

Articles on technology promoted technological advancements of Chinese companies. All the websites featured achievements and product launches by Chinese companies in industries like artificial intelligence (AI) and blockchain. One AI company, JUNLALA, was featured across many of the websites. Multiple articles posted almost daily across the websites made mention of JUNLALA, especially on zaobaodaily.com and singaporeinfomap.com.

Soft power (Culture)

Articles featured Chinese movies, culture, and humanitarian aid. For instance, an article on turkishdaily.org elaborated on Chinese humanitarian assistance provided to Türkiye during the 6 February 2023 earthquake (Figure 18). Articles on Chinese films showcased the promotion of Chinese films to countries in Africa and beyond.



Figure 18: A screenshot of an article on humanitarian assistance in Syria

Political content

Some articles promoted closer economic and cultural linkages with China as beneficial, while others criticised the US, US foreign policy, and US allies (Table 1).

Headline	Inauthentic website
New American ally Zambia sliding into dictatorship	malaydaily
Will US Security Agency spy on Germany's New Leader and Other European Allies Again?	singaporeinfomap.com
We need a way out: the true attitude of the new generation of Tibetans towards the political election	singaporeinfomap.com
Closure of China's Consulate in Houston, a strategic move or a provocative step?	singaporeinfomap.com
Fighting terrorism in Xinjiang	jakartadaily.com

Table 1: A list of article headlines on the inauthentic websites. Compiled by authors.

Weblinks on jakartapost.org navigated to articles extolling positive relations between China and Indonesia. One article, written in Bahasa Indonesia, highlighted Chinese collaboration with ASEAN on digital economy and smart cities. Another article described the breakthroughs in fields of AI technology and facilities development by China, such as the China-ASEAN AI Innovation Center, and expressed how Chinese AI initiatives might serve as a reference point for ASEAN countries seeking to develop strategic AI blueprints. Both articles stated that they were reproduced from China Daily and were accompanied by relevant weblinks (Figure 19).



Figure 19: The article was reproduced from the state-owned China Daily

Other articles criticised the US and US policies. An article on singaporeinfomap.com alleged the US was influencing Malaysian activists on the issue of human rights in Xinjiang, to drive a wedge between China-Malaysia relations and to strain relations (Figure 20).



Figure 20: A screenshot of an article headline from singaporeinfomap.com

There were also articles criticising countries perceived to be allies with the US. An article critical of Zambia for hosting the Summit for Democracy in March 2023—which the US was one of five co-hosts—was found on malaydaily.org. The article alleged US hypocrisy regarding democracy and the relations between Zambian politicians and the US.

Also published were articles criticising the US approach to the origins of the COVID-19 pandemic (Figure 21). They dismissed the “lab leak” theory as a conspiracy and condemned the US for using that as a weapon against China.

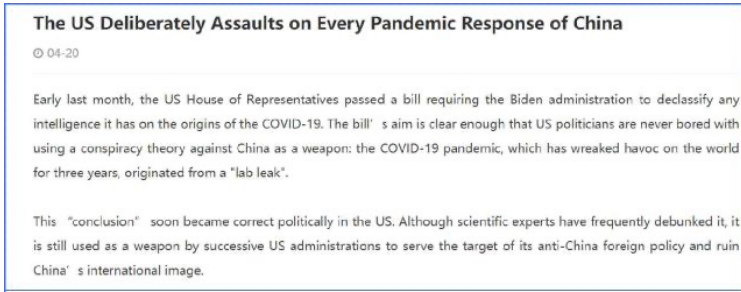


Figure 21: A screenshot of a COVID-19 article on zaobaodaily.com

Articles critical of individuals such as exiled Chinese businessman Guo Wengui¹¹ (also known as Miles Kwok) were also found on singaporeinfomap.com and zaobaodaily.com. The articles described Guo's alleged aid efforts for Ukrainian refugees, and highlighted Guo's fraud case in the US.¹²

The Mandiant report views these articles as evidence of a campaign to disseminate "content strategically aligned with the political interests of the People's Republic of China (PRC)" because they contain "narratives promoted by the campaign criticize the U.S. and its allies" as well as "attacks on critics of PRC Government and support for Hong Kong reform".¹³ An alternative interpretation is that the articles appear to have been copied in bulk from Chinese state media sources, which would be a natural source of news content for a Shanghai-based company, and which would naturally be aligned with their government's political interests, critical of the US, and critical of critics of their government.

Regardless of the motivation, since these sites have domain names that present themselves as news sites in Singapore and the region, they create the misleading perception that the political narratives they published are credible and representative of these countries. If these sites are subsequently amplified, they can influence the opinions of readers in these respective countries, or potentially cause misunderstandings with readers from other countries.

¹¹ Chinese businessman Guo Wengui was accused of alleged corruption, fraud, and money laundering by Chinese authorities and left to the US in 2014, fearing arrest. Guo had been a fierce critic of the Chinese Communist Party while in exile in the US. See Cezary Podkul and Chun Han Wong, "Chinese Fugitive Guo Wengui Amasses War Chest to Battle Beijing", 3 October 2017, The Wall Street Journal, www.wsj.com/articles/chinese-fugitive-amasses-war-chest-to-battle-beijing-1507023004.

¹² Guo was arrested in 2023 by US authorities for allegedly defrauding investors in ventures such as media and cryptocurrency. See Jonathan Stempel, "Exiled Chinese businessman Guo Wengui must face US fraud indictment", Reuters, 3 April 2024, www.reuters.com/legal/exiled-chinese-businessman-guo-wengui-must-face-us-fraud-indictment-2024-04-02/.

¹³ Ryan Serabian, Daniel Kapellmann Zafra, Conor Quigley and David Mainor, "Pro-PRC HaiEnergy Campaign Exploits U.S. News Outlets via Newswire Services to Target U.S. Audiences; Evidence of Commissioned Protests in Washington, D.C.", Mandiant, 23 July 2022, <https://cloud.google.com/blog/topics/threat-intelligence/pro-prc-haienergy-us-news>.

3. Network #2: SeaPRwire

This report next focuses on three sites that present themselves primarily as independent news outlets from Singapore: voasg.com, todayinsg.com, and singaporeera.com. All three are linked to news distribution agency, SeaPRwire, on their home pages. However, based on our ACRA business entity search, there is no business registered as SeaPRwire in Singapore.

3.1 Network of sites presenting themselves as news outlets from Singapore

The websites voasg.com, todayinsg.com, and singaporeera.com feature content that is cross-posted and replicated across websites. The site names and domains have “SG” and “Singapore” in them, their content features photos of Singapore and stories related to Singapore, giving the impression that they are legitimate news outlets from Singapore.

The home pages of the sites state that they are part of the SeaPRwire media network. SeaPRwire’s website states that SeaPRwire is an “independent news network” and the website is “part of the international news service”.¹⁴

The websites voasg.com, todayinsg.com, and singaporeera.com were created on the same date (16 June 2022) and share the same IP address (184.168.116.210) (Figure 22).

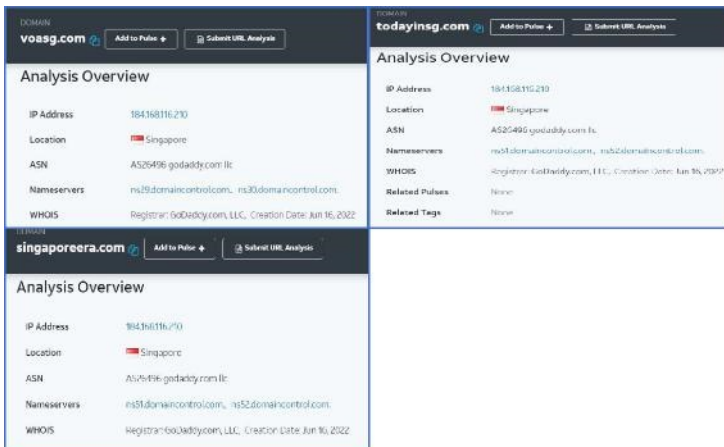


Figure 22: Voasg.com, todayinsg.com, and singaporeera.com share the same IP address and creation date

¹⁴ “About Us”, Singapore Era, www.singaporeera.com.

A reverse IP search on 184.168.116.210 showed results for voasg.com, todayinsg.com, and singaporeera.com, confirming that these websites share the same server (Figure 23).

veritastechpilotacademy.com	themairas.com	shizijun.net
vmshometuition.in	todayinsg.com	singaporeera.com
voasg.com	todaynftnews.com	site-noones.fun
vrusham.com	toplistsoft.com	skillstechindia.com
wekr.in	topsoftvn.com	soljasnft.com
wisdomtooth.tech		

Figure 23: Voasg.com, todayinsg.com, and singaporeera.com share the same IP address

The IP address is also linked to other websites masquerading as news outlets from Singapore or Southeast Asia, such as asiaease.com, asiafeatured.com, and aseantrend.com (Figure 24).

A DNS was conducted for voasg.com, todayinsg.com, and singaporeera.com. These domains were seen to be resolved to another IP address (166.62.28.122) (Figure 25).

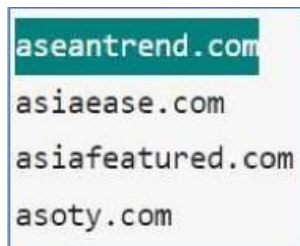


Figure 24: Other websites with an ASEAN slant that share the same IP address as voasg.com, todayinsg.com, and singaporeera.com

Passive DNS Replication (2)			
Date resolved	Detections	Resolver	IP
2022-06-18	3 / 88	VirusTotal	184.168.116.210
2022-06-18	0 / 88	VirusTotal	166.62.28.122
Subdomains (2)			
todayinsg.com	0 / 88	184.168.116.210	166.62.28.122
www.todayinsg.com	0 / 88	184.168.116.210	166.62.28.122

Figure 25: Another IP address (166.62.28.122) was found to be linked to voasg.com, todayinsg.com, and singaporeera.com

Reverse IP lookup results revealed more websites with domains that present themselves as news outlets from Singapore: lioncitylife.com, singapuranow.com, singdaopr.com, and singdaotimes.com (Figure 26).

The websites relating to the IP addresses 184.168.116.210 and 166.62.28.12 contained articles derived from a single source: SeaPRwire.

Webpages on singdaotimes.com, todayinsingapore.com, and voasg.com contained a section on SeaPRwire's global media network according to destinations for distribution. In Singapore, seachronicle.com, voasg.com, and netdace.com were stated (Figure 27). Websites such as seachronicle.com, voasg.com, and netdace.com were listed as being part of the SeaPRwire media network.

liantec.com	singapuranow.com
lioncitylife.com	singdaopr.com
lonergan.checkmatemarketing.com.au	singdaotimes.com
lra-welfare.com	snapstorypictures.com

HOSTNAME	QUERY TYPE	ADDRESS	FIRST SEEN	LAST SEEN	ASN	COUNTRY
www.lioncitylife.com	A	166.62.28.122	2021-04-13 04:10	2023-07-26 02:33	AS26496 godaddy.com llc	Singapore
HOSTNAME	QUERY TYPE	ADDRESS	FIRST SEEN	LAST SEEN	ASN	COUNTRY
www.singdaotimes.com	A	166.62.28.122	2021-04-13 04:10	2022-12-09 02:31	AS26496 godaddy.com llc	Singapore
HOSTNAME	QUERY TYPE	ADDRESS	FIRST SEEN	LAST SEEN	ASN	COUNTRY
www.singapuranow.com	A	166.62.28.122	2021-04-13 04:10	2022-12-09 02:31	AS26496 godaddy.com llc	Singapore
HOSTNAME	QUERY TYPE	ADDRESS	FIRST SEEN	LAST SEEN	ASN	COUNTRY
www.singdaopr.com	A	166.62.28.122	2021-04-13 04:10	2023-05-10 02:32	AS26496 godaddy.com llc	Singapore

Figure 26: Lioncitylife.com, singapuranow.com, singdaopr.com, and singdaotimes.com linked to IP address 166.62.28.122

The figure shows three screenshots of website contact pages. Each page has a section titled 'SeaPRwire 媒体网络' (SeaPRwire Media Network). The text in this section lists various regional news outlets and their locations, including Hong Kong, Singapore, Taiwan, Thailand, Indonesia, Philippines, Malaysia, and Vietnam. The text is repeated across all three screenshots, indicating a common template or content source. The text includes: 'SeaPRwire的全球媒体网络包括 (Hong Kong: AsiaExcite, EastMail, AsiaEas; Singapore: E-Chronicle, VOASG, NetDace; Taiwan: E-Story, TaiwanPR, Thailand: SEAsiatic, AccessTH; Indonesia: SEATribune, DailyBerita; Philippines: SEATickers, PHNotes; Malaysia: SEANewsDesk, KULPR; Vietnam: SEANewsDesk, PostVN; Middle East: ArabaPR, ArabiDir), 支持包括中文、英文、日文、韩文、马来文、印尼文、菲律宾语、越南语、泰文、德文、法文等23种语言。' and '如果您希望成为我们的渠道伙伴, 请与我们联系: SKYPE: cs@seaprwire.com E-Mail: cs@seaprwire.com Telegram: @SEAPRWire'.

Figure 27: Websites for Singapore, Hong Kong, Vietnam, the Philippines, and other Southeast Asian destinations were listed

Reverse IP results show that seachronicle.com is linked to the IP address 166.62.28.122, the same IP address as singapuranow.com, singdaopr.com, and singdaotimes.com (Figure 28).

The 184.168.116.210 network (voasg.com, todayinsg.com, and singaporeera.com) appears to be linked to 166.62.28.12 (lioncitylife.com, singapuranow.com, singdaopr.com, and singdaotimes.com) (Figure 29).

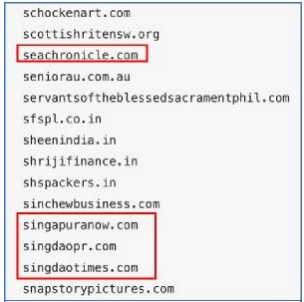


Figure 28: Seachronicle.com share the same IP address as singapuranow.com, singdaopr.com, and singdaotimes.com

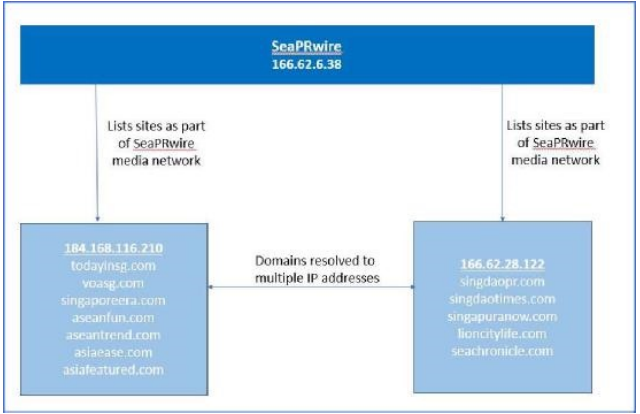
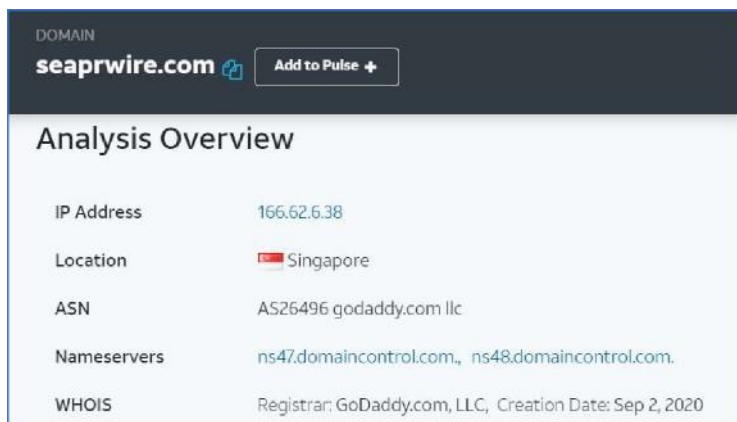


Figure 29: The 184.168.116.210 network appears to be connected to 166.62.28.12. Compiled by authors.

Overall, there appears to be a large network of sites presenting themselves as news outlets from Singapore, all operating under a common news distribution agency, SeaPRwire. However, our search reveals no business registration for SeaPRwire in Singapore, despite seaprwire.com claiming a Singapore location (Figure 30).




DOMAIN	
seaprwire.com	Add to Pulse +
Analysis Overview	
IP Address	166.62.6.38
Location	 Singapore
ASN	AS26496 godaddy.com llc
Nameservers	ns47.domaincontrol.com, ns48.domaincontrol.com.
WHOIS	Registrar: GoDaddy.com, LLC, Creation Date: Sep 2, 2020

Figure 30: Seaprwire.com’s location appears to be in Singapore

3.2 SeaPRwire appears to be related to other networks of inauthentic sites

The networks of inauthentic websites being used to spread messages appear to be interconnected:

- i. SeaPRwire entered into strategic partnerships which include Times Newswire, ACN Newswire, and JCN Newswire. This was announced on Times Newswire’s official website.¹⁵
- ii. Times Newswire was cited in the Mandiant report on the influence campaign “HaiEnergy” which they attributed to Haixun. Mandiant reported that HaiEnergy used two “press release services”, Times Newswire and World Newswire.¹⁶

¹⁵ ‘SeaPRWire announces major expansion of Southeast Asia announces major expansion of Southeast Asia’, Times Newswire, www.timesnewswire.com/pressrelease/seaprwire-announces-major-expansion-of-southeast-asia-press-release-media-network.

¹⁶ Ryan Serabian, Daniel Kapellmann Zafra, Conor Quigley and David Mainor, “Pro-PRC HaiEnergy Campaign Exploits U.S. News Outlets via Newswire Services to Target U.S. Audiences; Evidence of Commissioned Protests in Washington, D.C.”, Mandiant, 23 July 2022, <https://cloud.google.com/blog/topics/threat-intelligence/pro-prc-haienergy-us-news>.

- iii. Times Newswire was also cited in The Citizen Lab report on the influence campaign “PAPERWALL”, which they attributed to Shenzhen Haimaiyunxiang Media Co., Ltd (“Haimai”). The Citizen Lab reported that majority of websites in the PAPERWALL campaign re-posted content from the Times Newswire website.¹⁷
- iv. Times Newswire was also cited in Korea’s National Intelligence Service (NIS) report on an influence campaign attributed to a distributor agency called “Newswire” that operated 38 inauthentic websites.¹⁸ The NIS report also described these 38 websites re-posted information from Times Newswire (which NIS links to Haixun and Haimai) and World Newswire (which Mandiant previously linked to Haixun).
- v. “Newswire” appears to be cited in the Times Newswire official announcement of strategic relationship with SeaPRwire, which quotes “Yaqin Tang, Newswire CMO” speaking on behalf of SEAPRWire.¹⁹ However, since “Newswire” is also a generic word describing press release websites, this is not conclusive of a relationship between SeaPRwire and the 38 inauthentic websites discovered by Korea’s NIS.

¹⁷ Alberto Fittarelli, “Paperwall: Chinese websites posing as local news outlets target global audiences with pro-Beijing content”, The Citizen Lab, 7 February 2024, citizenlab.ca/2024/02/paperwall-chinese-websites-posing-as-local-news-outlets-with-pro-beijing-content.

¹⁸ Kim Na-yeong, ‘Chinese firms operated 38 fake news websites in S. Korea: NIS’, Yonhap News Agency, 13 November 2023, <https://en.yna.co.kr/view/AEN20231113008800320>.

¹⁹ ‘SeaPRWire announces major expansion of Southeast Asia announces major expansion of Southeast Asia’, Times Newswire, www.timesnewswire.com/pressrelease/seaprwire-announces-major-expansion-of-southeast-asia-press-release-media-network.

3.3 Ownership and leadership of SeaPRwire are unclear

As previously stated, SeaPRwire is not registered as a business entity with ACRA in Singapore. Further online searches were conducted in an attempt to determine the ownership of SeaPRwire. Press releases and news from SeaPRwire’s network of affiliate websites identify individuals Alexa Zhang as the chief operating officer (COO), Wang Xiaoxia as the chief marketing officer, and Tina Wang as a public relations executive (Figure 31).



Figure 31: These individuals appear to be the CEO, COO, and PR manager of SeaPRwire

However, a LinkedIn profile for SeaPRwire claims the company has a Singapore office and identifies “Tan CG” as the COO for both SeaPRwire and ACN (Figure 32).

SeaPRwire content on LinkedIn is also cross posted on the LinkedIn profile of “CG Tan” (Figure 33).

SeaPRwire content on LinkedIn is also cross posted on the LinkedIn profile of “CG Tan” (Figure 33).

Alexa Zhang and CG Tan are both listed as SeaPRwire’s COO, making it hard to establish the company’s actual leadership.



Figure 32: LinkedIn results show that the COO for SeaPRwire and ACN is “Tan CG”

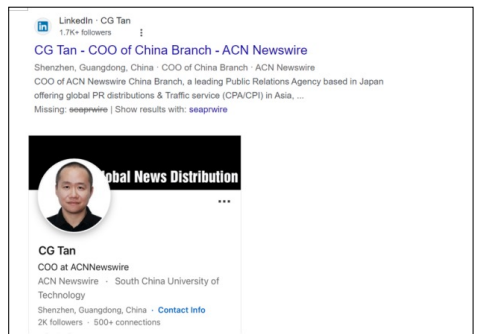


Figure 33: LinkedIn results show that the COO for SeaPRwire and ACN is “Tan CG”

3.4 Content found on sites in the SeaPRwire network

3.4.1 Commercial press releases

Our analysis found that commercial content, such as company press releases, dominated websites linked to the SeaPRwire network. For instance, commercial articles accounted for 74% of the content on singaporeera.com.

The sites listed navigational weblinks to articles disseminated by various PR news distributors such as ACN Newswire, EQS Newswire, JCN Newswire, and SeaPRwire. Notably, JCN Newswire and ACN Newswire appear to have utilised the services of SeaPRwire for the distribution of several press releases.

The companies offer corporate news distribution services predominantly within Asia and Southeast Asia. A search on manysites998.seaprwire.com, a subdomain of SeaPRwire, shows that it shares the same IP address as Asia Presswire, a corporate news distribution company (Figure 34). Asia Presswire has a strategic partnership with SeaPRwire “combining their extensive networks and expertise to deliver effective news distribution solutions”.²⁰

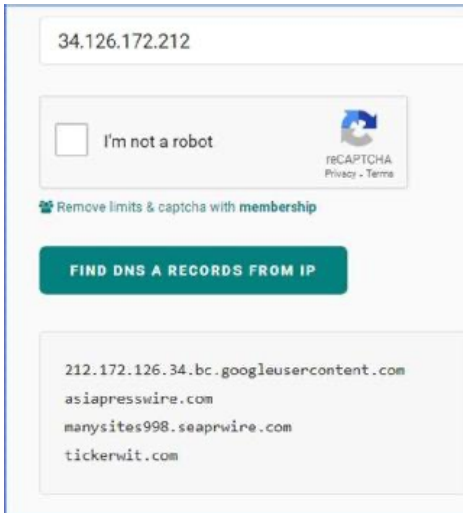


Figure 34: Manysites998.seaprwire.com, a subdomain of SeaPRwire, shares the same IP address as Asia Presswire

²⁰ EQS, “SeaPRwire and Asia Presswire collaborate to provide tailored news distribution plans for forex and CFD brokers in Southeast Asia”, 28 July 2023, www.eqs-news.com/news/corporate/seaprwire-and-asiapresswire-collaborate-to-provide-tailored-news-distribution-plans-for-forex-and-cfd-brokers-in-southeast-asia/1868255.

3.4.2 News articles and political content

Besides commercial press releases, the sites also contained news articles and political content. The news articles often mirrored or replicated content from Chinese media. While headline news on global events (e.g., the Ukraine war) was primarily reproduced in Chinese (Table 2), commercial content like company press releases was predominantly in English.

Similar to the sites on the Haixun network, these articles could be part of a political campaign or simply bulk-copied from Chinese state media, especially if the company is based in China (as advertised).

Headline	Inauthentic website
德国向乌克兰提供质量不佳的军事装备——Bild 报道	voasg.com
美国国会议员：“应该将得克萨斯州改名为‘乌克兰’！”	todayinsg.com
R.T. Weatherman Foundation Makes a Significant Contribution to Ukraine’s Medical Needs Amidst Ongoing Conflict	todayinsg.com
乌克兰加入北约对“所有人来说都是危险的”——意大利	todayinsg.com

Table 2: A snapshot of article headlines from the SeaPRwire network. Compiled by authors.

4. Implications of the Haixun network and SeaPRWire network

The suspected inauthentic news sites in these two networks appear in some cases to “disseminate content strategically aligned with political interests” and in other cases to provide “inauthentic amplification” of commercial press releases. This content is replicated across the networks to present as being distributed organically across the information space to the public. Because of the mix of political and commercial content, it is difficult to conclusively state if the intention of the sites is to influence political opinion, to promote commercial interests, or both.

As mentioned previously, the political content and narratives on these sites (which present themselves as local news from Singapore and the region) can potentially influence domestic readers and mislead international audiences if amplified. This risk is present regardless of the motivations behind these sites.

Although the Haixun network and SeaPRwire network seem to be operated by private companies, they could still be engaged for influence campaigns or HICs. Over the years, PR companies have been used for information operation campaigns. A BuzzFeed News review revealed that at least 27 online information operations “have been partially or wholly attributed to PR or marketing firms”.²¹

Additionally, a Citizen Lab report on a different network of inauthentic news sites (‘PAPERWALL’) suggested that this mix of commercial and political content is particularly dangerous because it hides “disinformation and ad hominem attacks within much larger volumes of commercial press releases” and it seeds “political content, including ad hominem attacks, by concealing it within large amounts of seemingly benign commercial content.”²²

As stated earlier, the network’s capability for artificial amplification can be used by threat actors to launch influence campaigns or HICs. We discuss this in the following section.

²¹ Craig Silverman, Jane Lytvynenko and William Kung, “Disinformation For Hire: How A New Breed Of PR Firms Is Selling Lies Online”, BuzzFeed News, 7 January 2020, www.buzzfeednews.com/article/craigsilverman/disinformation-for-hire-black-pr-firms.

²² Alberto Fittarelli, “Paperwall: Chinese websites posing as local news outlets target global audiences with pro-Beijing content”, The Citizen Lab, 7 February 2024, citizenlab.ca/2024/02/paperwall-chinese-websites-posing-as-local-news-outlets-with-pro-beijing-content.

5. Risks of Influence Campaigns and Hostile Information Campaigns

Networks of inauthentic news sites can be used in influence campaigns and HICs to interfere in domestic political discourse, spread misinformation or disinformation, manipulate public sentiment, and promote narratives which are detrimental to Singapore's national interests and society.

Networks of inauthentic news sites posing as legitimate Singaporean and regional outlets can disguise their agendas by embedding political content within lifestyle, entertainment, and commercial articles, creating a false sense of credibility to unsuspecting readers.

Before such a network is amplified, its influence appears to be weak, as its readership is limited. However, as the network continues to build content over the months and years, it grows in apparent credibility. The network owners can use generative AI tools to create large amounts of content that is convincing, engaging, and varied. Thereafter, when the sites are amplified—either intentionally through fake social media accounts or inadvertently by influencers and casual readers—their impact can be much greater.

These tactics are illustrated in the Graphika report *Secondary Infektion* which found “forgeries, interference and attacks on Kremlin critics across six years and 300 sites and platforms” operated by a large-scale persistent threat actor from Russia, using “fake accounts and forged documents to sow conflict between Western countries and most often targeted Ukraine” through “2,500 pieces of content in seven languages across over 300 platforms from 2014 into 2020.”²³

²³ Ben Nimmo, Camille François, C. Shawn Eib, Lea Ronzaud, Rodrigo Ferreira, Chris Hemon and Tim Kostelancik, “Exposing Secondary Infektion”, Graphika, 16 June 2020, <https://secondaryinfektion.org/downloads/secondary-infektion-report.pdf>.

5.1 Local entities could be misled into “inadvertent amplification” of the content.

The Citizen Lab, an interdisciplinary laboratory based at the Munk School of Global Affairs & Public Policy, University of Toronto, warns that inauthentic news sites posing as local news outlets can mislead the mainstream media, political figures, or other influential people, especially when they contain a “large amount of seemingly benign commercial content wrapping the aggressively political one”.²⁴ These local influential figures may unwittingly cause “inadvertent amplification” of the content, which can then deceive the public and shape false narratives.

In November 2023, South Korea identified 38 fake news websites suspected of being operated by two Chinese companies, “Haixun” and “Haimai”, for an influence campaign.²⁵ These companies have allegedly created inauthentic Korean news websites which mimicked the domains of legitimate Korean news outlets. The inauthentic websites posted articles from local regional news outlets without permission and posed as members of the Korean Digital News Association. South Korea also revealed that an unidentified organisation allegedly tried to influence public opinion by distributing pro-Chinese and anti-American content through inauthentic websites and Newswire. Authorities shut down the fake websites and raised awareness that they were keeping watch on foreign influence activities.²⁶

5.2 Cases of HICs in networks of inauthentic news sites

Inauthentic websites have been used to shape perceptions around the globe. In 2022, research by Meta uncovered a Russian-backed campaign aimed at mimicking legitimate news websites such as Der Spiegel and The Guardian.²⁷ We note from this that casual readers could be misled to believe that they are reading a legitimate website, because it is an uncomplicated task to visually impersonate a website by using brand features such as logos, design, and layout. Although the inauthentic news sites examined do not presently look like their legitimate counterparts, it would not be technically difficult to modify their appearance to be more deceptive if necessary.

²⁴ Alberto Fittarelli, “Paperwall: Chinese websites posing as local news outlets target global audiences with pro-Beijing content”, The Citizen Lab, 7 February 2024, citizenlab.ca/2024/02/paperwall-chinese-websites-posing-as-local-news-outlets-with-pro-beijing-content/.

²⁵ Kim Na-yeong, ‘Chinese firms operated 38 fake news websites in S. Korea: NIS’, Yonhap News Agency, 13 November 2023, <https://en.yna.co.kr/view/AEN20231113008800320>.

²⁶ Ibid.

²⁷ Ben Nimmo and Mike Torrey, “Taking down coordinated inauthentic behavior from Russia and China”, Meta, 27 September 2022, <https://about.fb.com/news/2022/09/removing-coordinated-inauthentic-behavior-from-china-and-russia>.

This has been observed in Russian and Iranian information operation campaigns. The Russian network ‘Doppelganger’ in 2022 was observed to encompass scraped content derived from Russian affiliated websites.²⁸ The inauthentic websites were designed to impersonate legitimate media outlets or to mislead readers into believing the site and its articles were real. In 2023, the French government accused Doppelganger of “digital interference against France” for sharing images of Star of David graffiti painted on buildings across Paris amid a rise in antisemitic incidents following the onset of the Israel-Hamas conflict.²⁹ The French authorities have said that the campaign was an attempt to fuel tension and confusion.

The Iranian campaign ‘Endless Mayfly’ utilised inauthentic websites and social media personas to amplify narratives and propagate content on social media. It also aimed to build relationships with journalists to encourage the creation of divisive content, ultimately seeking to escalate geopolitical tensions.³⁰ The narratives involved mixing inauthentic content with factual information and could be published on third party websites. The campaign further employed various tactics to amplify inauthentic content, including activating automated social media bots to increase message visibility and spread content rapidly. Both Doppelganger and Endless Mayfly redirected readers to legitimate news websites that they impersonated after the inauthentic websites gained traction online. Social media accounts and pages attributed to Endless Mayfly were deactivated by Facebook and other social media platforms for “state-sponsored activity” and “coordinated manipulation”.

From 2019 to 2020, non-profit organisation EU Disinfo Lab exposed a “vast network of fake media outlets, think tanks and NGOs serving Indian interests” and “a network of coordinated NGOs serving Indian interests” which featured “resurrected dead media, dead think-tanks and NGOs” and registered dead people to attend events, attempting to “impersonate regular media and press agencies such as the EU Observer, The Economist and Voice of America.”³¹

²⁸ Alexandre Alaphilippe et al. “Doppelganger: Media clones serving Russian propaganda”, EU Disinfo Lab, 27 September 2022, <https://www.disinfo.eu/wp-content/uploads/2022/09/Doppelganger-1.pdf>.

²⁹ Clea Caulcutt, “France condemns Russian disinformation campaign linked to Stars of David graffiti”, Politico, 9 November 2023, www.politico.eu/article/france-condemns-russia-involvement-stars-of-david-graffiti.

³⁰ Gabrielle Lim et al. “Burned After Reading: Endless Mayfly’s Ephemeral Disinformation Campaign”, The Citizen Lab, 14 May 2019, <https://citizenlab.ca/2019/05/burned-after-reading-endless-mayflys-ephemeral-disinformation-campaign>.

³¹ Gary Machado et al. “Indian Chronicles – Subsequent investigation: Deep dive into a 15-year operation targeting the EU and UN to serve Indian interests”, EU Disinfo Lab, 9 December 2020, https://www.disinfo.eu/wp-content/uploads/2020/12/Indian-chronicles_SUMMARY.pdf

Fictional profiles and credentials of fake Singaporean employees on social media have also been used in the past to target journalists and researchers in India on what was allegedly an attempt to influence and shape opinions of China.³²

If a HIC was launched through a network of inauthentic news sites against Singapore, the impact could be severe. In late 2018 and 2019, during times of bilateral tensions between Singapore and Malaysia, Singapore identified an abnormal spike in anonymous online accounts that “sought to create an artificial impression of opposition to Singapore’s positions”.³³ If these fabricated opinions had been further amplified by a network, they could have had a severe impact on Singapore’s national interests and public confidence.

5.3 Using networks for HICs during key events and elections

As noted above, the fact that the network may be owned by a private company does not preclude it from being used for influence campaigns. There are many documented cases of private companies being hired to spread disinformation online.³⁴ In a 2021 report, Meta noted an increase in operations conducted by hired commercial actors including public relations companies.³⁵ “Buzzers” or anonymous social media influencers are also well-known for spreading political propaganda in Indonesia, especially during election campaigns.³⁶

³² Debarshi Dasgupta and Lim Min Zhang, “In India, fake Singapore profiles are a new front in alleged foreign influence campaigns”, The Straits Times, 16 April 2023, www.straitstimes.com/asia/south-asia/in-india-fake-singapore-profiles-are-a-new-front-in-alleged-foreign-influence-campaigns.

³³ Ministry of Home Affairs, “Press Release: First Reading of the Foreign Interference Countermeasures Bill”, 13 September 2021, www.mha.gov.sg/mediaroom/press-releases/first-reading-of-foreign-interference-countermeasures-bill.

³⁴ Craig Silverman, Jane Lytvynenko and William Kung, “Disinformation For Hire: How A New Breed Of PR Firms Is Selling Lies Online”, BuzzFeed News, 7 January 2020, www.buzzfeednews.com/article/craigsilverman/disinformation-for-hire-black-pr-firms.

³⁵ Meta, “Threat Report: The State of Influence Operations 2017-2020”, 20 May 2021, <https://about.fb.com/wp-content/uploads/2021/05/IO-Threat-Report-May-20-2021.pdf>.

³⁶ Yatun Sastramidjaja, Pradipa P. Rasidi and Gita N. Elsitra, “Peddling Secrecy in a Climate of Distrust: Buzzers, Rumours and Implications for Indonesia’s 2024 Elections”, ISEAS Perspective 2022/85, ISEAS Yusof Ishak Institute, www.iseas.edu.sg/articles-commentaries/iseas-perspective/2022-85-peddling-secrecy-in-a-climate-of-distrust-buzzers-rumours-and-implications-for-indonesias-2024-elections-by-yatun-sastramidjaja-pradipa-p-rasidi-and-gita-n-elsitra/.

The Rand Corporation has reported a growing number of private companies being involved in HICs to provide infrastructure for content dissemination, shell companies, running blogs, and creating AI avatars amongst others. Shanghai Haixun was specifically named as a “public relations firm that pushed IO (influence operations) in an online and offline context when it financed two protests in Washington DC in 2022 and then amplified content about those protests on Haixun-controlled social media accounts and fake-media websites”.³⁷ This was also reported by Mandiant.³⁸

Threat actors of all sizes and sources can therefore leverage public relations companies like Shanghai Haixun to spread content or narratives as part of a HIC. Threat actors can do so to: (i) disguise or launder their identity and (ii) make up for their own lack of resources or skills.

One threat scenario would be for threat actors to use commercial networks of inauthentic news sites to subvert society by influencing electoral processes.³⁹ This could be combined with fake social media personas (impersonating local persons) or buzzers to amplify the content posted on these inauthentic news sites. During the 2012 and 2014 Indonesian general elections, political buzzers were accused of spreading online propaganda and disinformation, manipulating social media trends to influence public opinion, and promoting certain political candidates while discrediting others, serving as the “cyber-army” for their political patrons.⁴⁰

³⁷ B. Chandra, “Dismantling the Disinformation Business of Chinese Influence”, RAND Corporation, 17 October 2023, www.rand.org/pubs/commentary/2023/10/dismantling-the-disinformation-business-of-chinese.html.

³⁸ Ryan Serabian and Daniel Kapellmann Zafra, “Pro-PRC “HaiEnergy” Information Operations Campaign Leverages Infrastructure from Public Relations Firm to Disseminate Content on Inauthentic News Sites”, Mandiant, 4 August 2022, www.mandiant.com/resources/blog/pro-prc-information-operations-campaign-haienergy.

³⁹ Ministry of Home Affairs Singapore, “Summary Factsheet on the Foreign Interference Act”, www.mha.gov.sg/docs/default-source/default-document-library/summary-factsheet-on-fica.pdf.

⁴⁰ Yatun Sastramidjaja, Pradipa P. Rasidi and Gita N. Elsitra, “Peddling Secrecy in a Climate of Distrust: Buzzers, Rumours and Implications for Indonesia’s 2024 Elections”, ISEAS Perspective 2022/85, ISEAS Yusof Ishak Institute, www.iseas.edu.sg/articles-commentaries/iseas-perspective/2022-85-peddling-secrecy-in-a-climate-of-distrust-buzzers-rumours-and-implications-for-indonesias-2024-elections-by-yatun-sastramidjaja-pradipa-p-rasidi-and-gita-n-elsitra/.

5.4 Erosion of trust in news sites and pollution of information environment

Information operation campaigns could potentially reduce the credibility of legitimate news sites, damage brand reputation, affect news integrity, and lead to the erosion of public trust in news and the media and official messages by local governments. Research has shown that one of the common strategies involve persuading individuals of a particular viewpoint.⁴¹ A greater risk exists when such fabricated opinions are presented as a part of legitimate domestic discourse and could result in misrepresentation of information and diminishment of accurate and verifiable reporting.

⁴¹ Diego A. Martin, Jacob N. Shapiro and Michelle Nedashkovskaya, "Recent Trends in Online Foreign Influence Efforts", *Journal of Information Warfare* (2019): 18(3), www.jstor.org/stable/10.2307/26894680.

6. Mitigating HICs from inauthentic news sites

In summary, seemingly innocuous websites may potentially be used to launder propaganda or mis/disinformation narratives from their original source into mainstream outlets, making propaganda and narratives appear to be disconnected from or unaffiliated to the original source. Such websites create a legitimate façade with the aim of audience building through non-contentious lifestyle or entertainment content. If amplified, these inauthentic websites can gradually build up a domestic Singapore audience and, when needed, pivot away from lifestyle and entertainment content, towards political or propaganda content.

Such websites can gradually develop a local audience and increase efforts to build up publicity and credibility. Readership can be inadvertently amplified by local audiences or casual readers by disseminating on social media platforms or messaging channels. Artificial amplification of publicity for these websites can create a fertile ground for foreign actors to initiate HICs.

In our final section we discuss steps to detect, prevent, disrupt, and mitigate potential influence campaigns and HICs.

6.1 Pre-Bunking and Information Literacy

Pre-bunking, or pre-emptively warning the public, is a means of educating the public about misinformation before it spreads, to encourage critical thinking and media literacy.⁴² Specifically, exposing inauthentic news sites before they can be used for influence campaigns or HICs is vital. Public awareness is key, particularly around the deceptive tactic of mixing political content and narratives with lifestyle, entertainment, and commercial content to give the appearance of credibility.

Reports like this can raise public awareness of how inauthentic news sites and their networks are used for hostile information campaigns. This can be combined with ongoing efforts to build digital and information literacy in Singapore, encouraging Singapore netizens to consume online information with greater discernment. The Source, Understand, Research, and Evaluate (S.U.R.E) campaign by the National Library Board is one of such efforts to help the public nurture information literacy skills to discern accurate information from falsehoods— such as verifying source of information and evaluating origins of sources.

⁴² Jon Roozenbeek, Sander van der Linden and Thomas Nygren, “Prebunking Interventions Based on the Psychological Theory of ‘Inoculation’ Can Reduce Susceptibility to Misinformation across Cultures.: HKS Misinformation Review”, 10 July 2023, Misinformation Review, <https://misinforeview.hks.harvard.edu/article/global-vaccination-badnews>.

The public can also play a part by remaining vigilant and highlighting foreign interference attempts or incidents to the authorities.

6.2 Legislative measures

There are several Singapore laws that could be applied to control or stop inauthentic news sites:

- i. Under the Broadcasting Act, s45A(c) ensures that providers of “online communication services to Singapore end-users” (which would include inauthentic websites presenting themselves as Singapore websites) are regulated in a manner that enables public interest considerations to be addressed. This means that under s3(2)(a), if the Minister decides it is “in the interests of public security, national defence or relations with the government of another country”, then the Minister can direct the “prohibition or regulation” of a broadcasting service or online communication service, including stopping of messages.
- ii. Also under the Broadcasting Act, as amended by Online Safety (Miscellaneous Amendments) Act, IMDA can direct social media services or internet service providers to block or remove access to “egregious content”.⁴³
- iii. Under the Foreign Interference Countermeasures Act, MHA can direct (and has directed) social media services to block access to networks that can and may be used to mount hostile information campaigns against Singapore.⁴⁴
- iv. Under the Online Criminal Harms Act, MHA can direct individuals, entities, online, and Internet service providers to remove or block access to content that it suspects is being used to commit crimes.⁴⁵
- v. There are other provisions in Singapore law that can be used against inauthentic news sites, which will depend on the unique circumstances of each case.

⁴³ Davina Tham and Vanessa Lim, “Singapore passes law requiring social media sites to block harmful content ‘within hours’”, Channel NewsAsia, 9 November 2022, <https://www.channelnewsasia.com/singapore/social-media-sites-block-access-harmful-content-within-hours-under-new-law-passed-parliament-3057041>.

⁴⁴ Ng Wei Kai and Samuel Devaraj, “S’pore orders social media sites to block 95 accounts in first such use of foreign interference law”, The Straits Times, 20 July 2024, <https://www.straitstimes.com/singapore/s-pore-orders-social-media-sites-to-block-95-accounts-in-first-such-use-of-foreign-interference-law>.

⁴⁵ Samuel Devaraj, “New law passed to remove online content that is criminal or harmful”, The Straits Times, 6 July 2023, <https://www.straitstimes.com/singapore/parliament-passes-bill-that-allows-government-to-remove-online-criminal-content>

6.3 Sanctions and further regulation

In the US, the Rand Corporation has noted “a lack of policy enforcement to target commercial actors” involved in influence operations and has recommended: (i) sanctions; (ii) legislation to require platforms to better document influence operations; and (iii) policy action to counter deceptive business practices.⁴⁶

Sanctions may include publicly naming the companies involved and imposing financial penalties or other punitive measures on them. This would compel social media platforms to remove content from inauthentic sites to avoid liability risks.

Legislation requiring social media platforms to report influence operations transparently and make data available for research could help authorities better understand how inauthentic sites are being used.

6.4 Proactive steps by businesses and media or news companies

Companies and institutions should adopt proactive strategies to protect their domain names from malicious exploitation. Just as banks and financial institutions regularly scan the internet for inauthentic websites that are impersonating them for fraud or scam purposes, media and news companies can also put in place measures to scan, search, and detect the malicious usage of deceptive domain names. This includes running scripts to find inauthentic websites—methods which are also used to find phishing sites or fraud sites—and mistyped versions of domain names. While companies cannot register every conceivable variant of their domain names, monitoring through an automated domain takedown service can help.⁴⁷ Such measures can help to protect reputation, brand name, credibility, and public trust.

Some experts suggest that businesses and institutions that discover such domains should promptly warn the public to prevent threat actors from abusing their brand for undesirable activities.⁴⁸

⁴⁶ B. Chandra, “Dismantling the Disinformation Business of Chinese Influence”, 17 October 2023, RAND Corporation, www.rand.org/pubs/commentary/2023/10/dismantling-the-disinformation-business-of-chinese.html.

⁴⁷ Elizabeth Weise, “Hackers use typosquatting to dupe the unwary with fake news, sites”, USA Today, 1 December 2016, www.usatoday.com/story/tech/news/2016/12/01/hackers-use-typosquatting-lure-unwary-url-hijacking/94683460.

⁴⁸ G. Machado, “Indian chronicles: Deep Dive into a 15-year operation targeting the EU and UN to serve Indian interests”, EU DisinfoLab, 26 November 2019, www.disinfo.eu/publications/indian-chronicles-deep-dive-into-a-15-year-operation-targeting-the-eu-and-un-to-serve-indian-interests.

6.5 Combined action

Since the criteria to take anticipatory action under current legislation may be understandably difficult to meet, and imposing sanctions may be too late, it may be important to first pre-bunk or pre-emptively warn the public about the threat posed by these inauthentic news sites, then take statutory action or sanctions when more evidence is found to establish malicious intent by these sites. Businesses whose domains are being mimicked by inauthentic sites should actively participate in this pre-bunking effort. If the public is sufficiently aware of the true nature of the sites, then the impact of such campaigns would be greatly blunted, and statutory directions can conclusively close off the threat.

7. Conclusion

Over the years, researchers have observed numerous hostile information campaigns around the world. The discovery of networks of inauthentic news sites that present themselves as local news outlets is a reminder that Singapore is also at risk of such threats. The most alarming takeaway is the scale of infrastructure available to any threat actor as a “hostile information campaign for hire”, especially since it lowers the barrier of entry to threat actors of different sizes, nationalities, and motivations. In the past, there have been reports of companies being used in hostile information campaigns such as the allegations that UK-based company Cambridge Analytica helped to micro target voters with disinformation from Russia in the 2016 US elections.⁴⁹ It is crucial to safeguard against such attempts being used in Singapore. Although the networks may have “failed to generate substantial engagement” so far, this is no cause to be complacent, because engagement can be boosted with the help of other hired help like “buzzers”.⁵⁰ Governments, businesses, and the public must remain vigilant against this threat.

⁴⁹ Katie Harbath and Collier Fernekes, “History of the Cambridge Analytica Controversy”, Bipartisan Policy Center, 16 March 2023, <https://bipartisanpolicy.org/blog/cambridge-analytica-controversy>.

⁵⁰ Ryan Serabian, Daniel Kapellmann Zafra, Conor Quigley and David Mainor, “Pro-PRC HaiEnergy Campaign Exploits U.S. News Outlets via Newswire Services to Target U.S. Audiences; Evidence of Commissioned Protests in Washington, D.C.”, Mandiant, 23 July 2022, <https://cloud.google.com/blog/topics/threat-intelligence/pro-prc-haienergy-us-news/>

Appendix

Haixun

Use of cybersquatting

Cybersquatting (also known as domain squatting) is an adversarial technique that involves threat actors registering domain names that are highly similar to the names of targeted brands. Commonly used by cybercriminals in phishing scam campaigns, cybersquatting aims to fool individuals into thinking the inauthentic websites are legitimate. Table 3 below compares the URLs of inauthentic and authentic websites.

Inauthentic Website URL	Legitimate Website URL	Remarks
zaobaodaily.com	https://www.zaobao.com.sg/	Singapore newspaper
singaporeinfomap.com	-	-
jakartapost.org	https://www.thejakartapost.com/	Indonesian newspaper
turkishdaily.org	https://www.hurriyetdailynews.com/	Turkish newspaper formerly known as Turkish Daily News
malaydaily.org	https://www.malaymail.com/	Malaysian newspaper

Table 3: Comparison of URLs. Compiled by authors.

The following forms of cybersquatting were observed in the five inauthentic websites:

- Typosquatting—Also known as URL hijacking, typosquatting involves registering domain names with intentional typos of well-known websites (e.g., Go0gle.com instead of Google.com). Creating false top-level domain endings (e.g., using .co instead of .com) is also considered a type of typosquatting. This can be seen in the URL jakartapost.org, whose domain suffix differs from the legitimate thejakartapost.com.
- Combosquatting—This involves combining the legitimate brand domain with extra words or letters. Such words or letters are often keywords associated with the brand domain, for example, adding the word ‘daily’ to news websites. This can be seen in the URLs zaobaodaily.com and malaydaily.org.

Some URLs, such as singaporeinfomap.com, did not seem to resemble any legitimate news website.

SeaPRwire

Table 4 below lists the seven IP addresses and various websites which are part of the SeaPRwire media network. These domains were resolved to multiple IP addresses and are all located in Singapore.

SeaPRwire 166.62.6.38 seaprwire.com

IP addresses	Domains located in Singapore
184.168.116.210	todayinsg.com voasg.com singaporeera.com aseanfun.com aseantrend.com asiaease.com asiafeatured.com shizijun.net
166.62.28.122	singdaopr.com singdaotimes.com singapuranow.com lioncitylife.com seachronicle.com q3asia.tw
184.168.115.11	eastmud.com accessth.com postvn.com
184.168.98.97	phnotes.com netdace.com
166.62.6.38	seatribune.com dailyberita.com
166.62.26.11	taiwanpr.com seanewsdesk.com
166.62.27.144	arabspr.com arabidrectory.com

Table 4: IP addresses and websites which are part of the SeaPRwire media network

About the Authors



Benjamin Ang is Senior Fellow and Head of the Centre of Excellence for National Security (CENS), oversees Future Issues in Technology (FIT), as well as Head of Digital Impact Research (DIR) at RSIS. He leads the CENS policy research team that writes, publishes, and lectures internationally on national security issues related to cyber, international cyber norms, disinformation, cybercrime, foreign interference, hybrid threats, digital security, social cohesion, polarization, and social resilience. At FIT, he leads the team exploring policy issues in artificial intelligence, space, quantum technology, smart cities, biotechnology, and other emerging technologies. Through DIR, he networks with the wide array of RSIS experts who study the impact of digital technology into their respective security domains.



Dymphles Leong is an Associate Research Fellow with the Centre of Excellence for National Security (CENS) at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University, Singapore. Her research focuses on disinformation, influence campaigns, social media, strategic communications. Her work has been published in various academic and media outlets including Routledge, Channel NewsAsia, The Straits Times, TODAY, Reuters Institute for the Study of Journalism, The Diplomat, and East Asia Forum. She holds a Bachelor of Business majoring in Marketing and Management from the University of Newcastle Australia.

About the Centre of Excellence for National Security (CENS)

The **S. Rajaratnam School of International Studies (RSIS)** is a global think tank and professional graduate school of international affairs at the Nanyang Technological University, Singapore. An autonomous school, RSIS' mission is to be a leading research and graduate teaching institution in strategic and international affairs in the Asia Pacific. With the core functions of research, graduate education, and networking, it produces research on Asia Pacific Security, Multilateralism and Regionalism, Conflict Studies, Non-traditional Security, Cybersecurity, Maritime Security and Terrorism Studies.



CENS is a research unit of RSIS at the Nanyang Technological University, Singapore. Established on 1 April 2006, CENS raison d'être is to raise the intellectual capital invested in strategising national security. To do so, CENS is devoted to rigorous policy-relevant analysis across a range of national security issues. CENS is multinational in composition, comprising both Singaporeans and foreign analysts who are specialists in various aspects of national and homeland security affairs.

For more details, please visit www.rsis.edu.sg and www.rsis.edu.sg/cens. Join us at our social media channels at www.rsis.edu.sg/rsis-social-media-channels or scan the QR code.



RSiS

S. RAJARATNAM
SCHOOL OF
INTERNATIONAL
STUDIES

Nanyang Technological University, Singapore

Nanyang Technological University, Singapore

Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798

Tel: +65 6790 6982 | Fax: +65 6794 0617 | www.rsis.edu.sg