Ponder the Improbable since 1996

INAUTHENTIC LOCAL LIFESTYLE AND NEWS WEBSITES AND THE CHALLENGE FOR MEDIA LITERACY

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

INAUTHENTIC LOCAL LIFESTYLE AND NEWS WEBSITES AND THE CHALLENGE FOR MEDIA LITERACY

Benjamin Ang
Dymples Leong

October 2024

Table of Contents

Executive Summary

A previous report on networks of inauthentic news sites and the risk of hostile information campaigns (HICs) in Singapore described websites that “present themselves primarily as independent news outlets from different regions across the world” but (in fact) originate from a single operator or owner in one location. This report highlights the risks of similar networks with potential to be used for HICs.

Websites that present themselves as local lifestyle or current affairs sites (hereafter “Local Lifestyle and News Websites”) pose special challenges to media literacy.

i. The first rule of media literacy is to examine the source of information. It was relatively easy to identify websites that provided unreliable content. The source would look suspicious because it would be full of conspiracy theories and extreme opinions.

ii. However, Local Lifestyle and News Websites which contain mostly ‘benign’ or ordinary lifestyle or current affairs/news stories do not raise suspicion in this way. Consequently, items of disinformation appearing on these websites may also appear to be innocuous and convincing.

iii. The reader will have to carry out deeper research to determine if there are other areas of concern, or facts that create suspicion, such as the identity (or anonymity) of the owner. This does not mean that every website with anonymous owners is a suspicious website.

We applied the Source, Understand, Research, and Evaluate (S.U.R.E.) framework of media literacy on four websites presenting as local Singapore news sites: Mothership, The Independent, The Online Citizen, and Alamak.io.

We observed that the author’s qualifications and publication history of one of them – Alamak.io – was unknown. We then used open-source tools to further investigate the provenance of this website but were unable to identify the owners. This raised further questions about the website, such as its true country of origin, its use of AI-generated content, and its business model or motivation. These findings do not conclusively indicate that the website is used for information manipulation, but they indicate that further observation is merited, for example if the website starts to feature content relating to Singapore’s politics.

Singapore is vulnerable to foreign interference through online HICs because it is “open”, highly digitally connected, and diverse society.

a. There are several Singapore laws that could be applied to control or stop inauthentic news sites, such as the Broadcasting Act or the Foreign Interference Countermeasures 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.

b. Readers cannot assume that a website that appears to be a benign and accurate local news site is trustworthy but will need to be judicious about the information it puts out and look deeper into its provenance.

Inauthentic websites such as Alamak.io demonstrate how a lack of transparent ownership and author attribution can enable foreign actors to mislead and misinform audiences on the source and the intention of articles from websites purporting to be ‘news’ sites. While the website presents itself as an independent website based in Singapore and covers local content related to Singapore, it contains articles with a foreign political angle. This can be potentially utilised to manipulate public sentiment with narratives which might be detrimental to Singapore, but there is no clear evidence of this so far.

1. Background

A previous report on networks of inauthentic news sites and the risk of hostile information campaigns (HICs) in Singapore described websites that “present themselves primarily as independent news outlets from different regions across the world” but (in fact) originate from a single operator or owner in one location. The report highlighted the risks of similar networks with potential to be used for hostile information campaigns.

Previous cases of inauthentic news sites have also been uncovered in Italy and South Korea. Six websites posed as Italian news outlets and were not registered in the national registry, as required for news outlets operating in Italy. The investigation, led by the Italian newspaper Il Foglio, alleged that the websites were operated by China.[1] In South Korea, eighteen websites posing as Korean-language websites, linked to Chinese public relations companies Haixun and Haimai, were flagged by the South Korean National Cyber Security Center. The websites also posed as members of the Korean Digital News Association. It was revealed that the inauthentic websites attempted to manipulate public opinion by distributing pro-Chinese and anti-American content.[2]

The authors were interested to find out if there were any other websites which used corresponding strategies and tactics similar to the Haxiun and SeaPRwire networks (i.e., usage of public relations agencies or news distribution agencies to artificially amplify and disseminate strategic content on their websites, and the risks of potential usage in hostile information campaigns.

More specifically, the authors were keen to discover if there were other websites with a mix of news, current affairs, lifestyle, and culture content focused on Singapore that could be used for information manipulation.

[1] “La fabbrica dei contenuti pro Cina”, Il Foglio, 25 October 2023, www.ilfoglio.it/esteri/2023/10/25/news/la-fabbrica-dei-contenuti-pro-cina-5826677/amp/.

[2] “Influence activities exploiting fake websites of Chinese media outlets”, National Cyber Security Center, 13 November 2023, www.ncsc.go.kr:4018/main/cop/bbs/selectBoardArticle.do?bbsId=SecurityAdvice_main&nttId=88028&menuNo=020000&subMenuNo=020200&thirdMenuNo=.

2. Information Manipulation

Information manipulation can be described as attempts to shape public opinion and attitudes through the online information space. Information manipulation can involve the use of new and traditional media to disseminate information which could be used to exploit and amplify societal divides in a target country or population.[3]

AI-generated news and information websites

The rise in news websites powered by AI-generated news is concerning. NewsGuard, an organisation which rates news and information websites, found over 300 sites it classified as "unreliable AI-generated news and information websites". Such websites contained generic web names, however, content on the websites were found to contain false claims and fabrications such as COVID-mis- and disinformation. The websites were also found to have published large number of articles – in the hundreds – on a wide range of topics such as "politics, technology, entertainment, and travel".[4] AI has been used by both state and non-state actors in influence operations. In 2024, OpenAI published a report revealing how actors utilised generative AI such as ChatGPT to support the gathering and analysing of data on potential targets for information manipulation. The websites tracked by NewsGuard had substantial portions of content which were produced by AI and did not disclose that it had AI-generated content. Content on the websites was presented in a way an "average reader could assume that its content is produced by human writers or journalists, because the site has a layout, generic or benign name, or other content typical to news and information websites".[5]

[3] Cybersecurity and Infrastructure Security Agency (CISA), "Information Manipulation", www.cisa.gov/sites/default/files/publications/information_manipulation_infographic_508.pdf.

[4] "Tracking AI-enabled Misinformation: Over 1000 'Unreliable AI-Generated News' Websites (and Counting), Plus the Top False Narratives Generated by Artificial Intelligence Tools", NewsGuard, 28 August 2024, www.newsguardtech.com/special-reports/ai-tracking-center/.

[5] "Disrupting deceptive uses of AI by covert influence operations", OpenAI, 30 May 2024, https://openai.com/index/disrupting-deceptive-uses-of-AI-by-covert-influence-operations/.

Disinformation can be propagated through benign-looking news websites

In March 2024, The New York Times reported that Russian websites had appeared, targeting the US by having names suggesting that they were local US news sites: D.C. Weekly, the New York News Daily, the Chicago Chronicle, and the Miami Chronicle. There are no such US local news organisations; researchers suggest they were meant to mimic actual news organisations and promote Russian propaganda by interspersing it among stories about crime, politics, and culture.[6]

This tactic has also been detected in Europe, with the "Corona 24 News" collection of websites that are all constructed in a similar fashion. The "24 Group" network of websites publish a high volume of largely benign content translated into English, sourced from around the internet. Each site is vaguely titled to reflect a country or topical target audience, but just as in the US case above, none of these news outlets exist in the respective countries.[7]

Researchers suggest that the owners of "24 Group" have created an 'information laundering' system by republishing and integrating benign content from public sources[8]:

i. The copying of public content removes the need to hire staff to write articles.
ii. As the sites publish benign content, they do not get flagged as suspicious by search engines, so they get indexed as if they are real news sites.
iii. They may then be picked up by news aggregators or by users on social media.
iv. This enables threat actors to strategically publish disinformation on the sites, which can be picked up, indexed, and spread from a source (news aggregator, social media user) that is separate from the original publisher.[9]

[6] Steven Lee Myers, "Spate of Mock News Sites with Russian ties pop up in U.S.", New York Times, 7 March 2024, www.nytimes.com/2024/03/07/business/media/russia-us-news-sites.html.

[7] Max Glicker and Clint Watts, "24 Group: How Obscure News Sites Selectively Spread Pro-Kremlin Disinformation", GMF, 25 February 2021, https://securingdemocracy.gmfus.org/24-group-how-obscure-news-sites-selectively-spread-pro-kremlin-disinformation/.

[8] This is the process of moving false or misleading information from a less credible source to a more credible one, to give the information more credibility – see https://www.poynter.org/fact-checking/2023/?how-russian-falsehoods-spread-to-the-us-through-faux-local-news/.

[9] Max Glicker and Clint Watts, "24 Group: How Obscure News Sites Selectively Spread Pro-Kremlin Disinformation", GMF, 25 February 2021, https://securingdemocracy.gmfus.org/24-group-how-obscure-news-sites-selectively-spread-pro-kremlin-disinformation/.

The strategy of placing news articles on alternative fringe news sites has been observed in other countries. This tactic of information laundering was seen in the US. In 2020, Meta revealed that the Russian group Internet Research Agency (IRA) had conducted an influence operation by hiring Americans to write for an inauthentic news website, Peace Data. Fake personas generated using AI were also deployed to create a seemingly legitimate news organisation.[10]

Information laundering has been previously used to disseminate Russian propaganda. Yala News, a fringe website targeted at audiences in the Middle East, was found to publish articles containing Russian propaganda originating from Russian state-backed networks Sputnik.[11] Yala News was used as a medium to disguise the original source of articles from Sputnik.

Threat actors can impersonate respected news websites and amplify them through fake social media accounts

Threat actors were also found to have posted fake articles masquerading as legitimate stories from legitimate news sites. Meta reported this as a "Russian disinformation campaign attempting to undermine Western support for Ukraine".[12] This influence operation created more than 60 websites with domains that mimicked or spoofed well-respected news sites including the UK's Guardian newspaper, Germany's Der Spiegel, the US's The Washington Post and Fox News. They then published false stories that criticised Ukraine's President Volodymyr Zelensky and US policy on Ukraine.

The threat actors then spread links to these stories across social media platforms, using 1,600 inauthentic Facebook accounts, to audiences in Germany, Italy, France, the UK, and Ukraine.[13] These would be deceptive because the links appear at first glance to come from respected sources.[14]

[10] Donie O'Sullivan, "After FBI tip, Facebook says it uncovered Russian meddling", CNN Business,1 September 2020, https://edition.cnn.com/2020/09/01/tech/russian-troll-group-facebook-campaign/index.html.

[11] Hannah Gelbart, "The UK company spreading Russian fake news to millions", BBC, 4 April 2023, www.bbc.com/news/world-65150030.

[12] Alexander Martin, "Russians impersonate Washington Post and Fox News with anti-Ukraine stories", The Record, 29 August 2023, https://therecord.media/russians-fake-news-anti-ukraine.

[13] Ibid

[14] "Huge Russia-based Disinformation Network about Ukraine War Disabled", CBC, 7 September 2022, www.cbc.ca/news/world/russia-fake-news-facebook-meta-1.6597994.

Previous cases of purported ‘news sites’ have been reported. For instance, the US State Department in November 2023 identified a disinformation campaign across Latin America. They accused Russia of spreading disinformation and anti-NATO / anti-Ukraine propaganda, crafted to appear local and organic to audiences in Latin America, and laundered through an ecosystem of proxy websites and organisations which appear to be independent news.[15]

In 2016, BuzzFeed News identified more than 100 active US politics websites being run from Macedonia, some of which had hundreds of thousands of followers, and a Guardian report identified 150 similar politics sites. According to interviews with the Macedonian site owners, they posted false and misleading outrageous US political news stories, because these generated the most online attention from US readers, which in turn earned them the most revenue from online advertisers, at the expense of the readers who were misled into believing the stories came from genuine news sites, and who were consuming misinformation that outraged and polarised them.[16]

Inauthentic news sites raised in the examples above also utilised information laundering. Information laundering enables actors to utilise proxies to obscure origin and purpose. Information can be distorted from the original intent and framed to present false narratives. Disinformation and distorted narratives can be spread from fringe websites, through social media platforms as intermediaries, and weave its way into public discourse online. It can also be picked up by mainstream news media and further disseminated. Information laundering has been previously used to disseminate Russian propaganda. Yala News, a fringe website targeted at audiences in the Middle East, was found to publish articles containing Russian propaganda originating from Russian state-backed networks Sputnik. Yala News was used as a medium to disguise the original source of articles from Sputnik.

[15] “The Kremlin’s Efforts to Covertly Spread Disinformation in Latin America”, U.S. Department of State, 7 November 2023, www.state.gov/the-kremlins-efforts-to-covertly-spread-disinformation-in-latin-america/.

[16] Craig Silverman and Lawrence Alexander, “How Teens In The Balkans Are Duping Trump Supporters With Fake News”, Buzzfeed News, 4 November 2016, www.buzzfeednews.com/article/craigsilverman/how-macedonia-became-a-global-hub-for-pro-trump-misinfo.

Studies have identified that journalists and news sites play an important role in the propagation of misinformation, because of their “privileged, influential role in networks”.[17] This is especially for news sites that have “a reputation as a credible and trustworthy source of information” because this creates greater acceptance in social networks, both in person and online.[18]

The EU Disinfo Lab has identified cases where news sites are used to spread disinformation:[19]

i. Established news brands spreading disinformation (because of changes in circumstances), such as FranceSoir, formerly a distinguished French newspaper that went bankrupt for a while, and later became a source for conspiracy theories and anti-vax content.

ii. Online “media” outlets posing as credible sources to spread disinformation, such as Bonanza Media, which claimed to be an independent investigative platform from the Netherlands but was discovered to assist Russia’s military intelligence in spreading misleading information about the shooting down of aircraft MH17. Other examples include:

    a. France Libre 24, a French language media site managed covertly by a Polish far-right media network, to provide French audiences with false or polarising messages on identity, religion, security, and migration.

    b. Peace Data, an alleged global news organisation, which was actually a Russian information operation set up by the Russian Internet Research Agency (IRA) to spread disinformation ahead of the US Presidential Election in 2020.

[17] Max Glicker and Clint Watts, “24 Group: How Obscure News Sites Selectively Spread Pro-Kremlin Disinformation”, GMF, 25 February 2021, https://securingdemocracy.gmfus.org/24-group-how-obscure-news-sites-selectively-spread-pro-kremlin-disinformation/.

[18] Donie O’Sullivan, “After FBI tip, Facebook says it uncovered Russian meddling”, CNN Business,1 September 2020, https://edition.cnn.com/2020/09/01/tech/russian-troll-group-facebook-campaign/index.html.

[19] Hannah Gelbart, “The UK company spreading Russian fake news to millions”, BBC, 4 April 2023, www.bbc.com/news/world-65150030.

Once a piece of disinformation appears on a news site, a hostile information campaign can use trolls or bots to disseminate and amplify it on social media. Since the source is a news site, it would appear to have credibility. Because of this tactic of amplification, even news websites that usually have less than 50,000 visits per month, which would escape mainstream media attention, can quickly be leveraged and scaled up for a hostile information campaign.

Threat actors will also use ‘sleeper’ social media accounts that appear benign for years. Researchers found 48 Twitter accounts with local-sounding names like @MilwaukeeVoice and @Seattle_Post that shared localised news items but were linked to Russia’s Internet Research Agency. The accounts were “serving as sleeper accounts building trust and readership for some future, unforeseen effort,”[20] giving threat actors the capability “if at any given moment, they wanted to operationalize this network of what seemed to be local American news handles, they can significantly influence the narrative on a breaking news story”.[21]

Threat actors include domestic extremists from opposite ends of the political and ideological spectrum

Although foreign threat actors have been accused in many of these information laundering cases, there are also cases of US-based domestic extremists and partisan groups using the same tactics. In November 2022, NewsGuard identified 1,202 of what they called “pink slime” websites i.e. websites funded by partisan groups posing as independent local news publishers, apparently with the intention to deceive readers into trusting them as credible sources of information.[22]

[20] Alexander Martin, “Russians impersonate Washington Post and Fox News with anti-Ukraine stories”, The Record, 29 August 2023, https://therecord.media/russians-fake-news-anti-ukraine.

[21] Ibid.

[22] “Secretly Partisan-Funded Websites Posing as Independent Local News Sites On Verge of Outnumbering Daily Newspapers in the U.S.”, NewsGuard, 12 December 2022, www.newsguardtech.com/press/partisan-funded-websites-nearly-outnumber-daily-newspapers-in-us/.

The partisan sites posing as local news sites comprised five groups on the left and right ends of the US political spectrum: Courier Newsroom, Local Government Information Services, The Main Street Sentinel, The American Independent, and Metric Media.[23]

i. Metric Media group, a right-wing group, operated 1,079 “pink slime” sites as locally branded websites, with names such as the Kalamazoo Times, Mobile Courant, and Suffolk Reporter.

ii. Democrat operative David Brock[24] operated five “pink slime” websites as local sites spun off from the liberal blog, The American Independent i.e. The Arizona Independent, The Michigan Independent, The Ohio Independent, The Pennsylvania Independent, and The Wisconsin Independent, and published partisan content targeted at key voting states.[25]

[23] Ibid.

[24] Michael Scherer, “Hillary Clinton’s Bulldog Blazes New Campaign Finance Trails”, 10 September 2015, https://time.com/4028459/david-brock-hillary-clinton-media-matters/.

[25] “Secretly Partisan-Funded Websites Posing as Independent Local News Sites On Verge of Outnumbering Daily Newspapers in the U.S.”, NewsGuard, 12 December 2022, www.newsguardtech.com/press/partisan-funded-websites-nearly-outnumber-daily-newspapers-in-us.

3. The challenge that 'information' manipulation poses to media literacy

One of the most important countermeasures against hostile information campaigns and foreign interference has been media literacy. The widely used framework for media literacy in Singapore is the S.U.R.E. framework from the National Library Board, Singapore, which has been promoted to schools, workplaces, and the community. The S.U.R.E. framework is as follows:[26]

- SOURCE: Identify the type of source – is it trustworthy? Check the author's qualifications and publication history to determine the origins.
- UNDERSTAND: Are they mostly facts or opinions? If they are opinions, do they come from experts who have the knowledge to support their view?
- RESEARCH: Use various platforms to go beyond the initial source. Review the information against multiple sources.
- EVALUATE: Are there content biases?

This framework is very useful for identifying websites that provide unreliable content. If a site is full of conspiracy theories and extreme opinions, then it would be considered a suspicious source. However, if a website contains mostly 'benign', ordinary lifestyle or news stories, especially including local stories that are mostly factually correct, then it would appear to be a trustworthy source.

[26] "S.U.R.E. Elevated", National Library Board Singapore, accessed [date of access], https://sure.nlb.gov.sg/resources/school-curriculum/advanced/part1-sure/.

S.U.R.E. FRAMEWORK	APPLICATION TO INFORMATION LAUNDERING SITES
SOURCE	
Identify the type of source – is it trustworthy?	If the content on the site is mostly accurate local news and cultural events, which can be corroborated with other news websites, then it will appear trustworthy.
Check the author's qualifications and publication history to determine the origins	If the author is anonymous and the ownership of the site is unclear or unknown, then it could be suspicious. If the site has been publishing benign and accurate content for several years, then it will appear trustworthy.
UNDERSTAND	
Are they mostly facts or opinions?	If the content on the site is mostly accurate local news, cultural events, sports, which can be corroborated with other news websites, then they are mostly facts, not opinions, and would appear trustworthy.
If they are opinions, do they come from experts who have the knowledge to support their view?	If the site contains original opinions sourced from credible experts (whose identities can be verifiable online), it might appear trustworthy. If the site contains opinions that are copied or adapted from expert statements in other publications, then it would appear trustworthy.
RESEARCH	
Use various platforms to go beyond the initial source. Review the information against multiple sources.	At this stage, if the reader searches for other sources to corroborate or fact check the story, then he/she may discover that the story is inaccurate or biased.
EVALUATE	
Are there content biases?	At this stage, if the reader detects content biases in the story, then he/she may decide not to trust its contents. However, if the story is published amidst many other stories on the site that are not biased, then the other stories would give it an appearance of legitimacy.

This means that readers cannot rely on first impressions of the source to assess these websites, but instead must use more detailed information literacy techniques.

In the following sections, we have selected four websites that appear online as local Singapore lifestyle and news sites (i.e. they feature lifestyle or news articles that include and revolve around local Singapore stories) and examined them using the information literacy techniques of the S.U.R.E. framework, to determine if there were any aspects of the sites that merited more detailed study. For ease of reference, we will refer to these sites as “Local Lifestyle and News Websites”.

We observed that the author’s qualifications and publication history of one of them was unknown. We then used open-source tools to further investigate the provenance of this website.

4. Analysis of websites presenting as local Singapore news sites

For this study, we compared four Local Lifestyle and News Websites in Singapore (Table 1). These websites had a mix of current affairs, news, and lifestyle content focused on Singapore.[27]

	Mothership	The Independent	The Online Citizen[28]	Alamak.io
At least one news article / month	Yes	Yes	Yes	Yes
Visitorship/ month	7.4M[29]	1.2M[30]	212.1K[31]	2.7K[32]
Owners	Bridgewater Holdings Pte Ltd[33]	The Independent News & Media Pte Ltd (formerly known as Protegesoft Pte Ltd)[34]	Terry Xu[35]	Not disclosed
Authors	Published in bylines	Published in bylines	Published in bylines	Mostly not disclosed

Table 1: Comparison table of four news websites.

Since the author's qualifications and publication history of Alamak.io were unknown, we conducted further study using open-source tools.

[27] See Appendix.

[28] The Online Citizen (TOC) has a new publication Gutzy Asia (https://gutzy.asia/) which focuses on news from Asia and Singapore. Gutzy Asia is based in Taiwan. The last article on TOC was published on 4 September 2023.

[29] Sum of all visits on desktop and mobile from the last month. "mothership.sg". Similarweb. Accessed 28 November 2023. https://www.similarweb.com/website/mothership.sg/#overview

[30] Sum of all visits on desktop and mobile from the last month. "theindependent.sg". Similarweb. Accessed 28 November 2023. https://www.similarweb.com/website/theindependent.sg/#overview

[31] Sum of all visits on desktop and mobile from the last month. "theonlinecitizen.com". Similarweb. Accessed 28 November 2023. https://www.similarweb.com/website/theonlinecitizen.com/#overview

[32] Sum of all visits on desktop and mobile from the last month. "alamak.io". Similarweb. Accessed 28 November 2023. https://www.similarweb.com/website/alamak.io/#overview

[33] Theresa Tan, "Charting his own course", NUS Office of Alumni Relations, www.nus.edu.sg/alumnet/thealumnus/issue-120/people/pursuit-of-excellence/charting-his-own-course.

[34] "About Us", The Independent Singapore, https://theindependent.sg/about-us/; "The Independent News & Media Pte. Ltd.", SGP Business, www.sgpbusiness.com/company/The-Independent-News-And-Media-Pte-Ltd.

[35] "About Us", The Independent Singapore, www.theonlinecitizen.com/about-us/.

Alamak.io

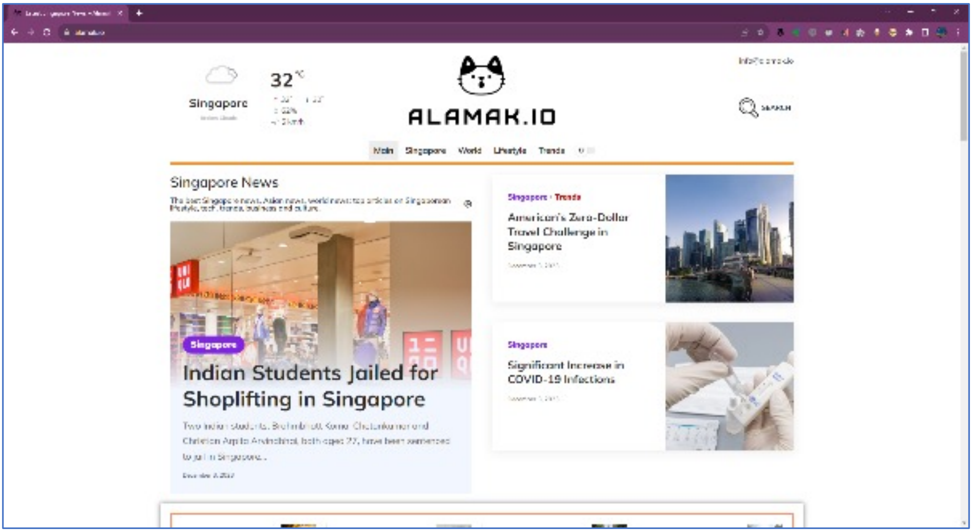

Singapore
32°C
ALAMAK.IO
SEARCH
Main
Singapore
World
Lifestyle
Trends
Singapore News
Singapore
Indian Students Jailed for Shoplifting in Singapore
Singapore · Trends
American's Zero-Dollar Travel Challenge in Singapore
Singapore
Significant Increase in COVID-19 Infections

Figure 1: Screenshot of Alamak.io

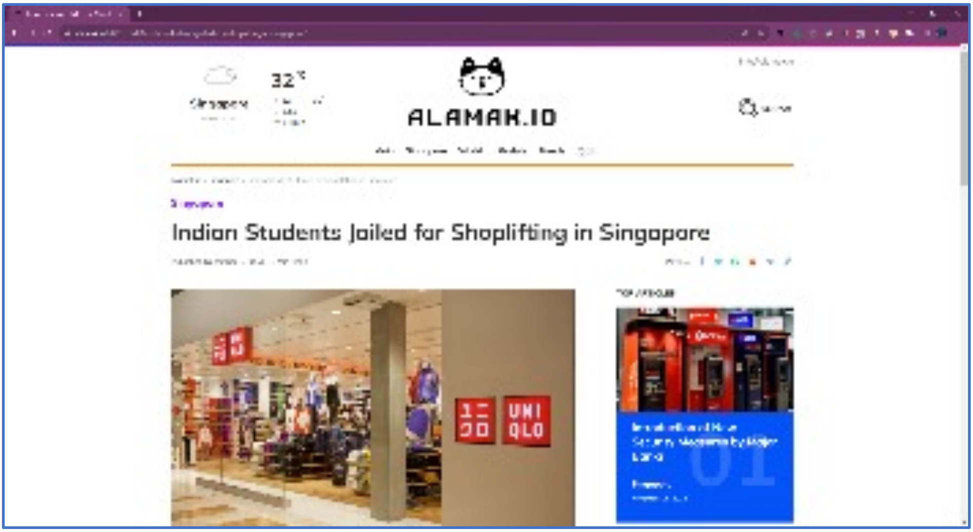
Alamak.io is a news website that features news articles on Singapore, covering current affairs, lifestyle, trends, and contributed opinions (Figure 1). Its ownership is unknown, unlike the other Local Lifestyle and News Websites, and is not available on the website.

Alamak.io utilised the colloquial word ‘Alamak’ as its website name. ‘Alamak’ is a colloquial word used in Singapore and Malaysia, often used as an interjection or expression to describe shock, worry, dismay, and disappointment. The usage of the term for the website appears to be intended to evoke familiarity and knowledge of the Singapore culture. It could also be so named to target at a Singapore or regional readership or demographic audience.

The authors are generally not identified in bylines (Figure 2).

There were only four contributed articles with a byline identifying the author (Figure 3).

Since Alamak.io does not disclose its ownership, we searched for this information using OSINT tools. The website was created on 24 March 2023 (Figure 4).



Singapore

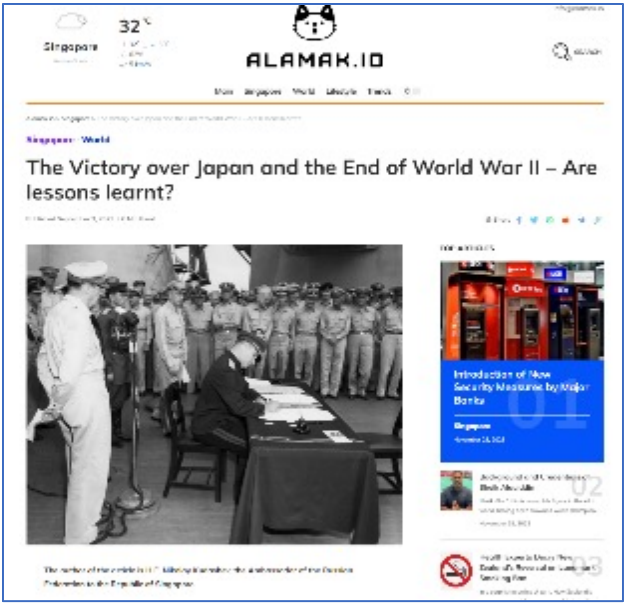
32°C

ALAMAK.IO

Singapore

Indian Students Jailed for Shoplifting in Singapore

Figure 2: Authors are generally not identified in bylines for Alamak.io



Singapore

32°C

ALAMAK.IO

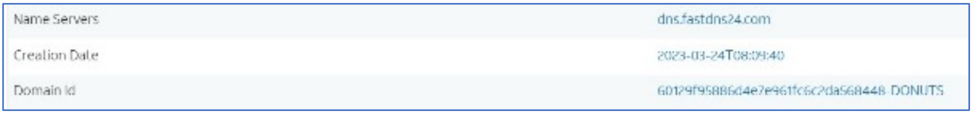
Singapore · World

The Victory over Japan and the End of World War II – Are lessons learnt?

Introduction of New Security Measures by Major Banks

Singapore

Figure 3: A screenshot of an article from Alaamk.io which has identifiable author stated



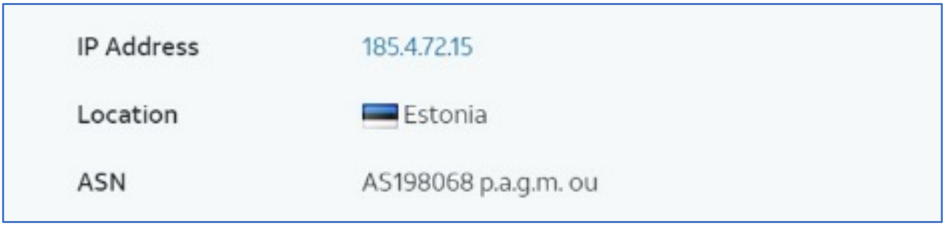
Name Servers	dns.fastdns24.com
Creation Date	2023-03-24T08:09:40
Domain Id	60129f95886d4e7e961fc6c2da568448-DONUTS

Figure 4: The website was created on 24 March 2023

A Domain Name System (DNS) search was conducted to map a domain to the physical IP address of the computer hosting that domain.[36]

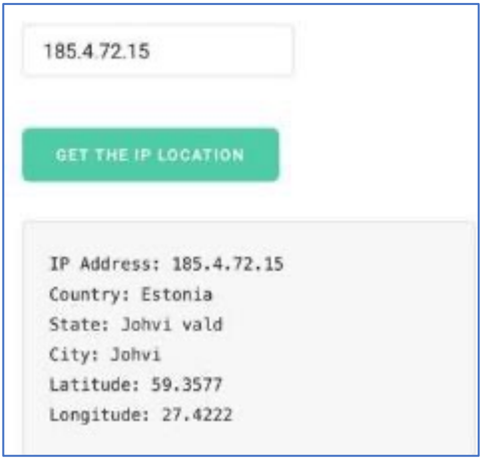
A search using both WHOIS and Alienvault revealed that the IP address for Alamak.io is 185.4.72.15. An IP geolocation search was conducted for the IP address 185.4.72.15. The IP address is seemingly located in Estonia (Figure 5).

A further search narrowed the location to be in Johvi, Estonia (Figure 6).



IP Address	185.4.72.15
Location	Estonia
ASN	AS198068 p.a.g.m. ou

Figure 5: IP address and location of the website



```
IP Address: 185.4.72.15
Country: Estonia
State: Johvi vald
City: Johvi
Latitude: 59.3577
Longitude: 27.4222
```

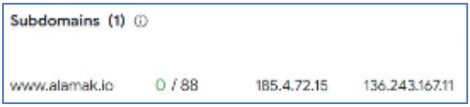
Figure 6: A further search revealed the location to be in the city of Johvi, Estonia

[36] DNS is the protocol that translates domain names into IP addresses and vice versa.

A search was also conducted to find all subdomains associated with Alamak.io. Results showed that a subdomain for Alamak.io is 136.243.167.11 (Figure 7).

A search was conducted to identify the DNS records from a primary domain name, in this case, Alamak.io. Results showed that it links to 5plus1.ru (Figure 8).

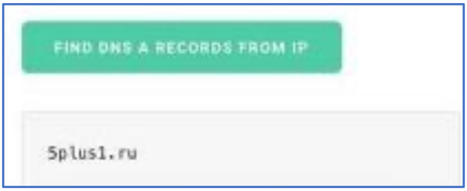
A reverse IP lookup is conducted to determine the records associated with an IP address. Reverse IP can also identify pinpoint virtual hosts served from a web server. The result revealed that the 5plus1.ru website is also associated with the IP address 185.4.72.15, the same IP address as Alamak.io (Figure 9).



Subdomains (1)

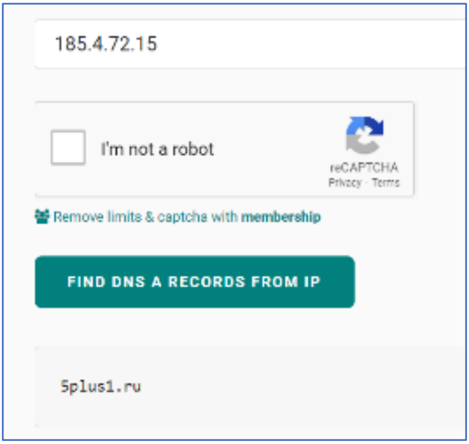
www.alamak.io	0 / 88	185.4.72.15	136.243.167.11

Figure 7: The subdomain for the website



```
5plus1.ru
```

Figure 8: Search for subdomains identified with the primary domain name Alamak.io



185.4.72.15

□ I'm not a robot
reCAPTCHA
Privacy · Terms
Remove limits & captcha with membership
FIND DNS A RECORDS FROM IP

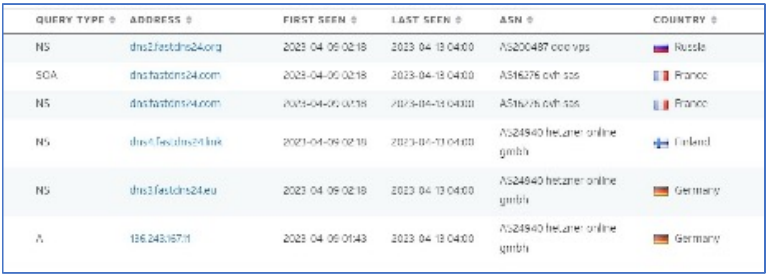
```
5plus1.ru
```

Figure 9: Reverse IP lookup reinforces the result that the IP address is linked to 5plus1.ru

An online search on 5plus1.ru shows it to be linked to 5+1 Media, a Russian communications agency. The website states that it was founded in 2018 by graduates and teachers from the Moscow State Institute of International Relations University of the Ministry of Foreign Affairs of the Russian Federation; and headed by founder Yuri Antsiferov.[37] The website, 5plus1.ru, lists various services such as targeted advertising, news monitoring, and website development. It lists completed projects in the fields of politics, Fast Moving Consumer Goods (FMCG) companies, energy, government, and tourism.[38]

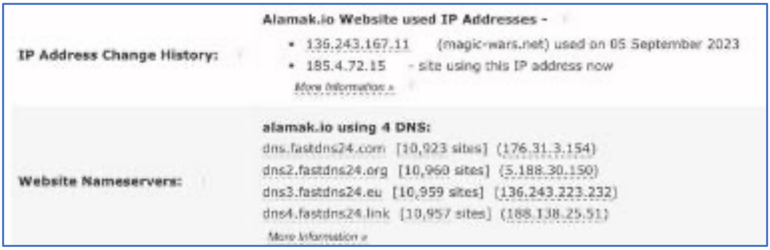
A check on various DNS associated with Alamak.io on Alienvault uncovered six passive DNS. Passive DNS records and stores historical DNS data for a given time or location. Passive DNS data can provide insight into how domain names change over time and to identify other related domains or IP addresses. The subdomain for Alamak.io 136.243.167.11 was created on 9 April 2023. It was last seen on 13 April 2023 (Figure 10).

A search revealed that the IP address for Alamak.io (185.4.72.15) was recently used. Previously it had used 136.243.167.11 and changed the IP address (Figure 11).



QUERY TYPE ⇕	ADDRESS ⇕	FIRST SEEN ⇕	LAST SEEN ⇕	ASN ⇕	COUNTRY ⇕
NS	dns2.fastdns24.org	2023-04-09 02:18	2023-04-13 04:00	AS200487 ooo vps	Russia
SOA	dns.fastdns24.com	2023-04-09 02:18	2023-04-13 04:00	AS16276 ovh sas	France
NS	dns.fastdns24.com	2023-04-09 02:18	2023-04-13 04:00	AS16276 ovh sas	France
NS	dns4.fastdns24.link	2023-04-09 02:18	2023-04-13 04:00	AS24940 hetzner online gmbh	Finland
NS	dns3.fastdns24.eu	2023-04-09 02:18	2023-04-13 04:00	AS24940 hetzner online gmbh	Germany
A	136.243.167.11	2023-04-09 01:43	2023-04-13 04:00	AS24940 hetzner online gmbh	Germany

Figure 10: Six passive DNS were linked to the website



IP Address Change History:	**Alamak.io Website used IP Addresses -** • 136.243.167.11 (magic-wars.net) used on 05 September 2023 • 185.4.72.15 - site using this IP address now More Information »
Website Nameservers:	**alamak.io using 4 DNS:** dns.fastdns24.com [10,923 sites] (176.31.3.154) dns2.fastdns24.org [10,960 sites] (5.188.30.150) dns3.fastdns24.eu [10,959 sites] (136.243.223.232) dns4.fastdns24.link [10,957 sites] (188.138.25.51) More Information »

Figure 11: The change in IP address for the website

[37] "5+1 Media", 5+1 Media, https://5plus1=ru.translate.goog/?_x_tr_sl=ru&_x_tr_tl=en&_x_tr_hl=en&_x_tr_pto=sc.

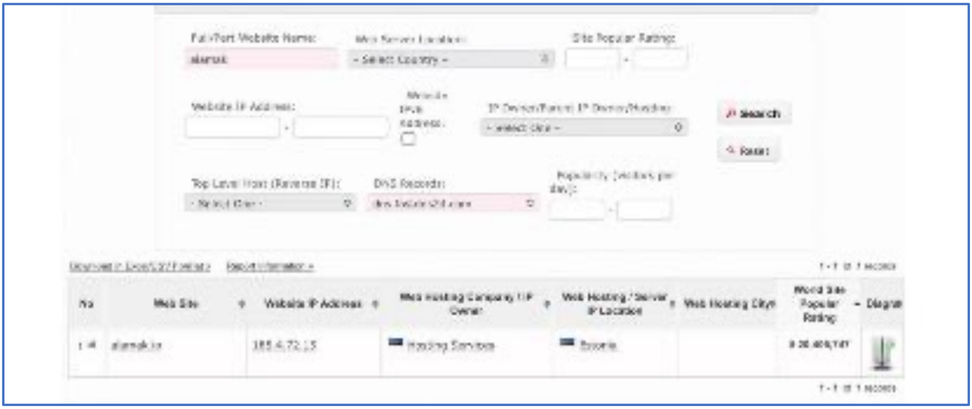
[38] Ibid.

A cross-check on the websites using the nameservers listed above confirms that Alamak.io is hosted on the nameserver dns.fastdns24.com (Figure 12).

Further cross-checks also revealed that Alamak.io is also confirmed to be hosted on the nameservers dns2.fastdns24.org, dns3.fastdns24.eu, and dns4.fastdns24.link (Figure 13).

Some other websites in Singapore were found to be hosted by the server. In this instance, a language school in Singapore used the same server (Figure 14).

A search on the subdomain IP address 136.243.167.11 revealed affiliation with a website, hexroast.com (Figure 15).



Full/Part Website Name: alamak

Web Server Location: - Select Country -

Site Popular Rating: -

Website IP Address: -

Website IPv6 Address: □

IP Owner/Parent IP Owner/Hoster: - select one -

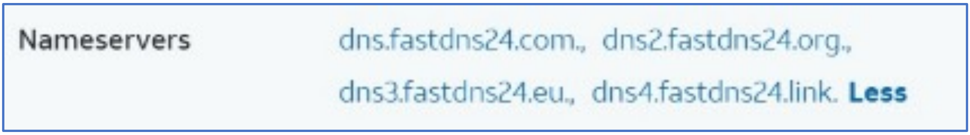
Top Level Host (Reverse IP): - Select One -

DNS Records: dns.fastdns24.com

Popularity (visitors per day): -

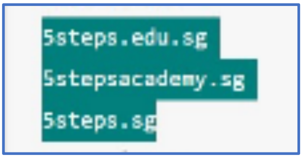
No	Web Site	Website IP Address	Web Hosting Company / IP Owner	Web Hosting / Server IP Location	Web Hosting City	World Site Popular Rating	Diagram
1	alamak.io	185.4.72.15	Hosting Services	Estonia		# 20,409,747	

Figure 12: Result showing link to the website and the nameserver



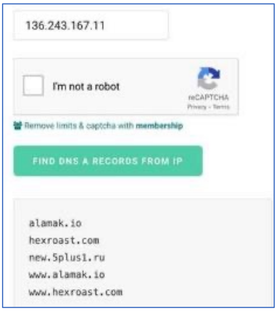
Nameservers dns.fastdns24.com., dns2.fastdns24.org., dns3.fastdns24.eu., dns4.fastdns24.link. **Less**

Figure 13: The four nameservers



5steps.edu.sg
5stepsacademy.sg
5steps.sg

Figure 14: Some websites using the same nameserver



136.243.167.11

☐ I'm not a robot

reCAPTCHA
Privacy - Terms
Remove limits & captcha with membership
FIND DNS A RECORDS FROM IP

```
alamak.io
hexroast.com
new.5plus1.ru
www.alamak.io
www.hexroast.com
```

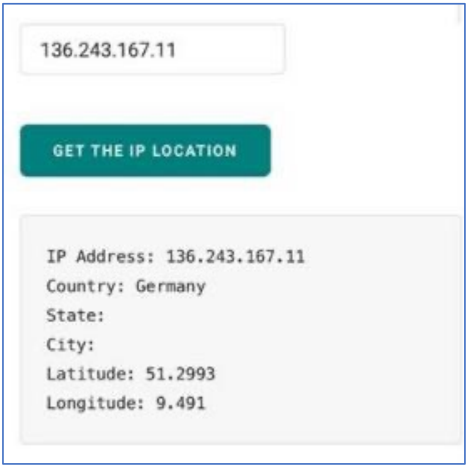
Figure 15: Hexroast.com is identified to be affiliated with the IP address

Results from a Google search revealed that hexroast.com appears to be an e-sports NFT game website. The game was promoted on social media platforms such as YouTube, LinkedIn, and Facebook. Press relation agencies such as MediaOnAsia were also utilised to disseminate news about the game. However, attempts to locate and access hexroast.com were unsuccessful. Attempts to access the hexroast weblink provided on social media promotions were also unsuccessful.

An IP geolocation search was also conducted for subdomain IP address 136.243.167.11. Search results revealed the alleged country location to be Germany (Figure 16).

A search was done to identify pictorial assets used on the website. Images appear to be uploaded to the website (Figure 17). Images on Alamak.io utilised analytics tracking code by Yandex, the largest search engine in Russia, indicative of pictorial assets being obtained from Yandex.

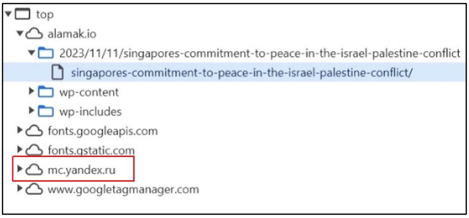
JPG pictures and photos were uploaded to be used for various articles on Alamak.io (Figure 18).



136.243.167.11

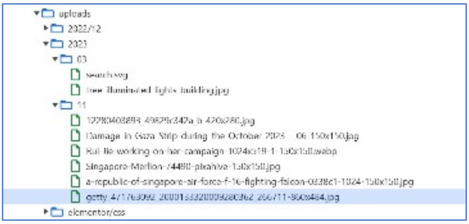
```
IP Address: 136.243.167.11
Country: Germany
State:
City:
Latitude: 51.2993
Longitude: 9.491
```

Figure 16: The IP address was traced back to Germany



```
▾ top
  ▾ alamak.io
    ▾ 2023/11/11/singapores-commitment-to-peace-in-the-israel-palestine-conflict
        singapores-commitment-to-peace-in-the-israel-palestine-conflict/
    ▸ wp-content
    ▸ wp-includes
  ▸ fonts.googleapis.com
  ▸ fonts.gstatic.com
  ▸ mc.yandex.ru
  ▸ www.googletagmanager.com
```

Figure 17: Pictorial assets used by the website

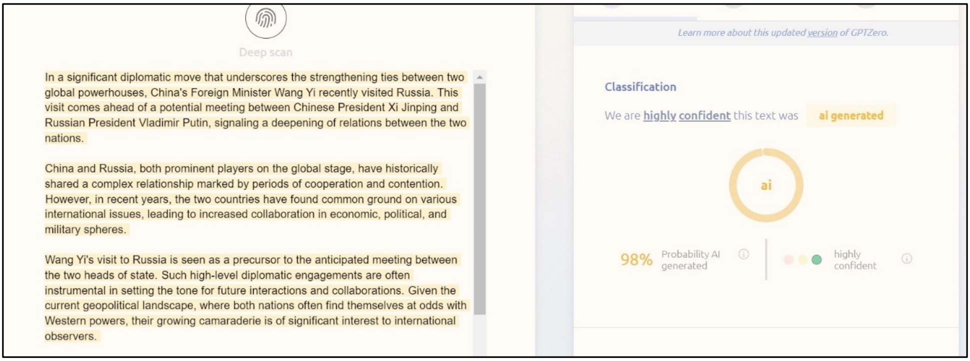


```
▾ uploads
  ▸ 2022/12
  ▾ 2023
    ▾ 03
        search.svg
        tree illuminated lights building.jpg
    ▾ 11
        12280403889_49829c342a_b 470x280.jpg
        Damage in Gaza Strip during the October 2023 06 150x150.jpg
        Rui-lie-working-on-her-campaign-1024x519-1-150x150.webp
        Singapore-Merlion-744801-pixahive-150x150.jpg
        a-republic-of-singapore-air-force-f-16-fighting-falcon-0338c1-1024-150x150.jpg
        getty 471763092 2000153320009280362 266711-900x484.jpg
  ▸ elementor/css
```

Figure 18: The names of the images used by the website

Based on the current information available through open-source tools, we were unable to conclusively identify the owners Alamak.io. Although the website primarily features Singapore news, we were unable to determine the website's ownership and funding and were unable to identify any Singapore-based sources of ownership and funding. We were only able to determine that the website is linked to entities in Germany, Estonia, and Russia.

Many articles on Alamak.io were seemingly generated or written by artificial intelligence (AI). For instance, the article titled "China's Wang Yi's Strategic Visit to Russia" was deemed by AI detection software to have a probability of 98% AI-generated text. Other articles were also deemed probable to have been generated by AI including "China Surpasses US as Leader in Branded Coffee Shops, Becoming a Global Powerhouse" (97% probability), "Philippines Denounces China's Use of Water Cannons in South China Sea Dispute" (98% probability) and "Singapore and China Announce 30-Day Visa-Free Travel to Boost Bilateral Ties" (98% probability).[39] This strongly suggests that the articles were AI-generated and raises questions about the lack of articles published by human authors on the website (Figure 19).



In a significant diplomatic move that underscores the strengthening ties between two global powerhouses, China's Foreign Minister Wang Yi recently visited Russia. This visit comes ahead of a potential meeting between Chinese President Xi Jinping and Russian President Vladimir Putin, signaling a deepening of relations between the two nations.

China and Russia, both prominent players on the global stage, have historically shared a complex relationship marked by periods of cooperation and contention. However, in recent years, the two countries have found common ground on various international issues, leading to increased collaboration in economic, political, and military spheres.

Wang Yi's visit to Russia is seen as a precursor to the anticipated meeting between the two heads of state. Such high-level diplomatic engagements are often instrumental in setting the tone for future interactions and collaborations. Given the current geopolitical landscape, where both nations often find themselves at odds with Western powers, their growing camaraderie is of significant interest to international observers.

We are highly confident this text was ai generated

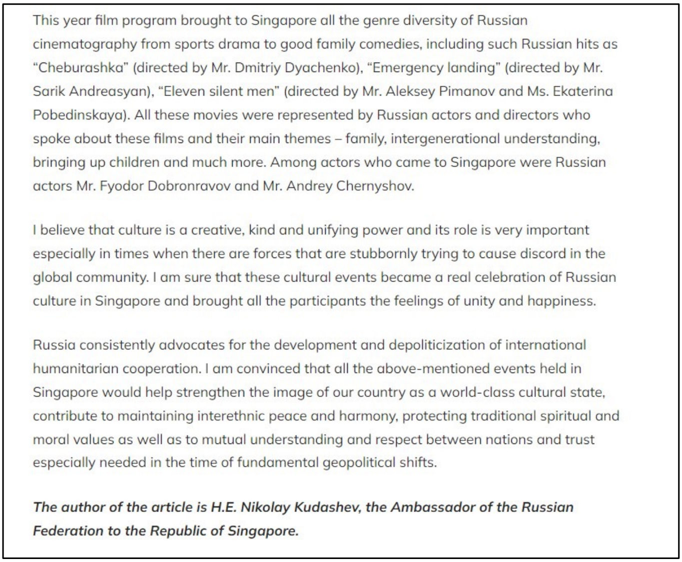
Figure 19: Some articles were seemingly generated by AI

[39] As computed by ZeroGPT.

We were also unable to identify the authors of the articles on Alamak.io, except for five articles with a byline as shown in Figure 20.

1. Russian diplomacy on the eve of the Second World War, published 8 May 2024, by H.E. Nikolay Kudashev, the Ambassador of the Russian Federation to the Republic of Singapore
2. Celebration of Russian Culture in Singapore, published 25 November 2023, by H.E. Nikolay Kudashev, the Ambassador of the Russian Federation to the Republic of Singapore
3. The Victory over Japan and the End of World War II – Are lessons learnt? published 3 September 2023 by H.E. Nikolay Kudashev, the Ambassador of the Russian Federation to the Republic of Singapore
4. Russia-ASEAN Cooperation: Navigating Challenges and Building a Strategic Partnership in a Multipolar World, published 8 August 2023, by H.E. Nikolay Kudashev, the Ambassador of the Russian Federation to the Republic of Singapore
5. The Future of Russia-ASEAN Relations: Unleashing Potential through Cooperation and Goodwill, published 12 June 2023, by H.E. Nikolay Kudashev, the Ambassador of the Russian Federation to the Republic of Singapore.

These articles were observed to be written and attributed to an author, allegedly the Russian Ambassador to Singapore (Figure 20).



This year film program brought to Singapore all the genre diversity of Russian cinematography from sports drama to good family comedies, including such Russian hits as "Cheburashka" (directed by Mr. Dmitriy Dyachenko), "Emergency landing" (directed by Mr. Sarik Andreasyan), "Eleven silent men" (directed by Mr. Aleksey Pimanov and Ms. Ekaterina Pobedinskaya). All these movies were represented by Russian actors and directors who spoke about these films and their main themes – family, intergenerational understanding, bringing up children and much more. Among actors who came to Singapore were Russian actors Mr. Fyodor Dobronravov and Mr. Andrey Chernyshov.

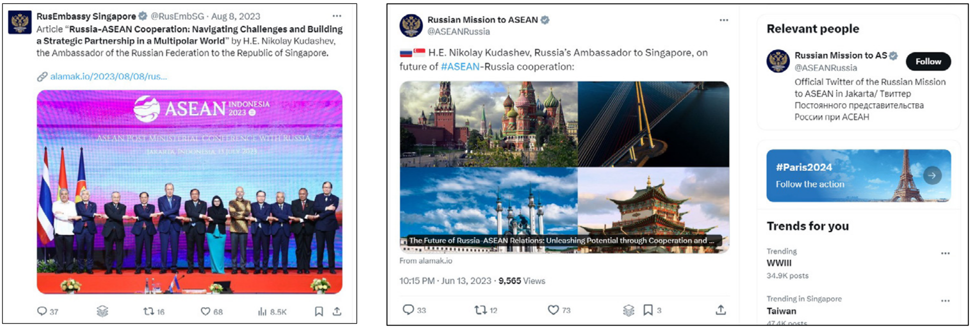
I believe that culture is a creative, kind and unifying power and its role is very important especially in times when there are forces that are stubbornly trying to cause discord in the global community. I am sure that these cultural events became a real celebration of Russian culture in Singapore and brought all the participants the feelings of unity and happiness.

Russia consistently advocates for the development and depoliticization of international humanitarian cooperation. I am convinced that all the above-mentioned events held in Singapore would help strengthen the image of our country as a world-class cultural state, contribute to maintaining interethnic peace and harmony, protecting traditional spiritual and moral values as well as to mutual understanding and respect between nations and trust especially needed in the time of fundamental geopolitical shifts.

The author of the article is H.E. Nikolay Kudashev, the Ambassador of the Russian Federation to the Republic of Singapore.

Figure 20: A screenshot of one of the five articles were observed to be written and attributed to an author, allegedly the Russian Ambassador to Singapore

There is corroboration that these articles were written by the Russian Ambassador to Singapore, as they were shared by the official Twitter (X.com) accounts of the Russian Embassy in the Republic of Singapore and the Russian Mission to ASEAN, and attributed to the Ambassador, as seen in the screenshots below.



RusEmbassy Singapore @RusEmbSG · Aug 8, 2023

Article "**Russia-ASEAN Cooperation: Navigating Challenges and Building a Strategic Partnership in a Multipolar World**" by H.E. Nikolay Kudashev, the Ambassador of the Russian Federation to the Republic of Singapore.

alamak.io/2023/08/08/rus...

ASEAN INDONESIA 2023
ASEAN POST MINISTERIAL CONFERENCE WITH RUSSIA
JAKARTA, INDONESIA, 13 JULY 2023

Russian Mission to ASEAN @ASEANRussia

🇷🇺🇸🇬 H.E. Nikolay Kudashev, Russia's Ambassador to Singapore, on future of #ASEAN-Russia cooperation:

The Future of Russia-ASEAN Relations: Unleashing Potential through Cooperation and ...

From alamak.io

10:15 PM · Jun 13, 2023 · **9,565** Views

Relevant people

Russian Mission to AS @ASEANRussia

Official Twitter of the Russian Mission to ASEAN in Jakarta/ Твиттер Постоянного представительства России при АСЕАН

#Paris2024
Follow the action

Trends for you

Trending
WWIII
34.9K posts

Trending in Singapore
Taiwan
47.4K posts

Figure 21: Posts on X.com by official Twitter accounts of the Russian Embassy in the Republic of Singapore and Russian Mission to ASEAN, sharing the abovementioned articles on Alamak.io and attributing them to Russia's Ambassador to Singapore

Finally, unlike the other Local Lifestyle and New Websites that we examined, there were no advertisements on Alamak.io. or calls for subscription. We were therefore unable to determine the business model or motivation for the website, because there is no indication of how and by whom it is funded.

In summary, we were unable to verify the author's qualifications and publication history to determine the origins of Alamak.io. Even though the site appears to be a Local Lifestyle and News Website, there is evidence that the owners and/or authors are not local, and some articles were authored by AI. We were also unable to determine how and by whom the website is funded.

These findings do not conclusively indicate that the website is used for information manipulation, but they indicate that further observation is merited, such as if the website starts to feature content relating to Singapore's politics or becomes part of an online hostile information campaign for foreign interference.

5. Application to Singapore

Singapore is vulnerable to foreign interference through online HICs because it is an "open, highly digitally connected, and diverse society".[40] In 2022, Taiwan-based research outfit Doublethink Lab ranked Singapore as the second most likely to be influenced by China in technology, society, and academia, but not domestic politics.[41] In 2021, French think-tank Institute for Strategic Research at France's Military College, or IRSEM, observed that Singapore was vulnerable to foreign interference, though it was "able to resist and defend against Chinese influence "skilfully".[42]

News websites can be used for foreign interference in various ways, such as spreading propaganda and disinformation to influence public opinion and undermine the credibility of the target country's government, institutions, and policies, or creating or amplifying divisive narratives and false claims to polarise the society and sow discord among different groups.[43]

If an established Singapore news website were to post disinformation or propaganda, the impact would be significant because of its reputation as a credible source of information. We further infer, from the case studies as raised above, that an online "media" outlet could pose as a credible Singapore source, with localised stories about Singapore media, to build its local credibility, but could subsequently be used to spread disinformation or false narratives or other inauthentic content. This content could in turn be disseminated and amplified on social media by bots and trolls. The creation and establishment of inauthentic news sites is a commonly identified Tactic, Technique, Procedure (TTP) used in a hostile information campaign. There is potential for inauthentic websites to gradually build up a following among Singapore audience and gradually pivot away from lifestyle and entertainment content, towards political or propaganda content.

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

[41] Justin Ong, "S'pore is second most influenced by China in the world, according to Taiwan report", The Straits Times, 4 May 2022, www.straitstimes.com/singapore/spore-is-second-most-influenced-by-china-in-the-world-according-to-taiwan-report; "Singapore", China Index, https://china-index.io/.

[42] Justin Ong, "Singapore particularly vulnerable yet resilient to Chinese influence operations: French report", The Straits Times, 2 October 2021, www.straitstimes.com/singapore/politics/spore-particularly-vulnerable-yet-resilient-to-chinese-influence-operations.

[43] "The beginner's guide to foreign interference", Channel NewsAsia, 27 September 2021, www.channelnewsasia.com/advertorial/beginners-guide-foreign-interference-2175361; "REPORT on foreign interference in all democratic processes", European Parliament, 15 May 2023, www.europarl.europa.eu/doceo/document/A-9-2023-0187_EN.html; "Foreign Interference Threats to Canada's Democratic Process", Government Of Canada, 22 July 2021, www.canada.ca/en/security-intelligence-service/corporate/publications/foreign-interference-threat-to-canadas-democratic-process.html.

Seemingly innocuous third-party websites may potentially be used to disseminate propaganda or mis/disinformation narratives from its original source, and publish them into the mainstream, making propaganda and narratives appear to be disconnected or unaffiliated to the original source. Such websites create a legitimate façade with the aim of audience-building through innocuous lifestyle or entertainment content.

Laws that can be applied

The Broadcasting Act regulates broadcasting services as well as “online communication services to Singapore end-users”, pursuant to s45A(c) which ensures that providers of “online communication services to Singapore end-users” are regulated in a manner that enables public interest considerations to be addressed. S45B further elaborates that the law applies to “any content that is provided on any online communication service and is accessible by any Singapore end-user”. This would cover news websites that are targeted at Singapore end-users.

Therefore, 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. S45I extends this to giving blocking directions to internet service providers, which would require them to stop access by Singapore end-users.

As an alternative step, s45K (1) provides that the Authority (IMDA) may designate an online communication service with a Singapore end-user link as a “regulated online communication service”. The website would then need to comply with regulatory requirements such as the prevailing Online Code of Practice, failing which the Authority could take regulatory action.

In cases where a website’s authorship or ownership are unknown, the Minister for Home Affairs may use the Foreign Interference (Countermeasures) Act (FICA) to issue a Technical Assistance Direction to a provider of a hosting service or a proprietor of an online location.

Under Section 36, “a technical assistance direction may require a person to whom the direction is given to do one or more of the following within the time specified in the direction, in relation to all or any of the person’s relevant activities: (a) to provide information about whether any account maintained by the person for a customer is that for a foreigner; (b) to provide technical information or other information about the person’s relevant activity as specified in the direction; (c) to take any other step directed towards ensuring that the person is capable of giving help to the competent authority which the competent authority requires in the public interest.”

If a website has been used for online communications that falls within the coverage of FICA, then pursuant to Section 20(1), the Minister can give an Access Blocking Direction if (a) there is undertaking of online communications activity, or online communications activity has been undertaken; (b) which is suspected of being or having been undertaken, by or on behalf of a foreign principal; (c) the online communications activity results in any information or material being published in Singapore; and (d) it is in the public interest.

The Access Blocking Direction under Section 33(2) requires the provider of an internet access service (e.g. ISP’s) to take all reasonable steps to disable access by every end-user in Singapore to the covered information or material (the website).

However, if a website (such as a Local Lifestyle or News Website as defined in this report) contains mostly benign or ordinary lifestyle or current affairs/news stories, then FICA would not apply, even though the website could potentially be pivoted to launch a hostile information campaign in future. In their current form, these provisions of FICA can only be applied when the undesirable activity has already taken place.

The Minister can also take Anticipatory Action under Section 21(1) if (a) a person is acting with the intention of preparing for, or planning to undertake, online communications activity by or on behalf of a foreign principal; (b) the Minister has reason to believe that, as a result of that online communications activity, information or material is likely to be published in Singapore; and (c) is of the opinion that it is in the public interest. However, Anticipatory Action can only be taken if all the above criteria are met, and it may be difficult to identify persons who are acting with the required intention, especially if the owners and authors of a website are unidentified. It would not be possible to use FICA in such a situation.

In view of these legislative gaps, it may be necessary to enhance the investigative powers of FICA to enable the authorities to identify owners and authors of Local Lifestyle and News Websites, and to provide or develop tools and resources to carry out digital forensics where needed. It may even be necessary to adjust the thresholds for application of FICA, but this must be done carefully to minimise the risk of taking action against innocent websites. Furthermore, if the public perceives that the application of FICA threshold is too low, there may be concerns that FICA can be abused and hence its effectiveness will be diminished.

Beyond legislative measures, there is a need to inoculate the public against HICs that come from inauthentic Local Lifestyle and News Websites. This may require exposing these sites to public scrutiny as well as publicising the tactics that have been employed in other countries.

Initiatives to nudge the public and encourage critical thinking and media literacy can be further highlighted to the public's attention. More specifically, greater awareness on potential tactics such as combining innocuous content such as news, lifestyle, and entertainment to give the appearance of credibility and authenticity. Ongoing initiatives such as the S.U.R.E. campaign by the National Library Board can help the public in understanding and developing information literacy skills to discern accurate information from falsehoods. A possible idea for consideration can include a brief explainer on some of the common tactics used for information manipulation for greater public awareness.

The need for vigilance

In the meantime, there will still be websites and social media accounts that present themselves as sharing local news with benign and even accurate news but have the potential to be used to share propaganda or worse, for HICs.

Since these sites appear at first look to be trustworthy, readers should carry out deeper research to determine if there are areas of suspicion, such as whether the owner is identified or anonymous. This does not mean that every website with anonymous owners is involved in information manipulation on a website. However, it does mean that readers need to be vigilant towards online sources of news that appear to originate from Singapore, and not assume that they are totally benign or accurate.

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.

Dymples 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