RSiS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS COMMENTARY

www.rsis.edu.sg

No. 162 – 23 October 2024

How a Network of Inauthentic Websites Could Be a Threat to Singapore

By Benjamin Ang and Dymples Leong

SYNOPSIS

On 22 October 2024, the Singapore Government issued directions to Singapore Internet service providers to disable access by its Singapore users to websites found to be "inauthentic". Such inauthentic websites are part of the new tactics being used in hostile information campaigns around the world, which could also be used against Singapore.

COMMENTARY

In recent years, as authorities and platforms worldwide take action against inauthentic social media accounts and websites that spread falsehoods and hate speeches, the threat actors behind them have changed their techniques to avoid detection.

One technique is to use networks of "inauthentic news" websites that "present themselves primarily as independent news outlets from different regions across the world" – as the cybersecurity and threat intelligence company Mandiant has put it – but are owned or operated in one location. This tactic was exposed in several reports by Mandiant, Citizen Lab (an academic research laboratory), and South Korea's National Intelligence Service, which identified several such networks used in foreign influence campaigns.

The threat posed by such websites has surfaced in Singapore, which could be used by foreign actors behind them to mount hostile information campaigns (HICs) here. Hence, the issuance of instructions on 22 October by the Ministry of Home Affairs (MHA) and the Infocomm Media Development Authority (IMDA) to Internet service providers to disable access by users in Singapore to ten websites identified as inauthentic.

The Threat Posed by Inauthentic Websites

These sites appear innocuous as they mostly feature non-controversial news on lifestyle and entertainment, but they are insidious for precisely that very reason. When the sites are used to spread disinformation or content serving the interest of foreign governments and agencies, the casual presence of non-controversial news gives them the cover that they need, i.e., the appearance of authenticity or credibility. The presence of a network comprising dozens of such sites, all repeating the same news stories, suggests corroboration to the unwary. It creates the "illusory truth effect", where repeated exposure to the same information increases its likelihood of being perceived as true, even when it is not.

Usually, most people are wary of websites that carry biased or unreliable information, such as those about vaccine conspiracies, climate change, or extreme ideologies. This is partly because of our sceptical nature and partly because of critical thinking and media literacy education programmes that teach us to evaluate the sources and reliability of information provided. However, website visitors could still be deceived into trusting inauthentic news sites, as most of the information they display is not obviously biased nor unreliable.

The action by MHA/IMDA to block access to inauthentic websites was not unexpected. Even before the issuance of the blocking order, an RSIS' team from the Centre of Excellence for National Security (CENS) had been observing dozens of sites in various networks with a view to publishing policy reports about them.

We found several suspicious news sites which falsely presented themselves as news outlets from Singapore and other Asian countries when they were found – as determined through open-source investigation methods and tools – to have links to a public relations company in Shanghai, which Mandiant had reported as being used for foreign influence campaigns.

There were other sites linked to a news distribution company (not registered in Singapore), with strategic links to a network of inauthentic news sites named in the South Korean and Citizen Lab reports as being used by foreign actors. Although there was one website where we could not identify the owner and the authors of the articles posted, we could tell from the online evidence that it was not from Singapore.

We found networks that were used to boost commercial press releases artificially. In one instance, a cryptocurrency business falsely claimed it had been cited in over a hundred news articles worldwide. In fact, it was a story replicated on a hundred sites in one of the networks to create the illusion of its global reach.

The inauthentic nature of these networks and sites allows a foreign actor to post a story, surround it with noncontroversial lifestyle or entertainment news, and make it appear to originate from different agencies and countries, even though it comes from a single source.

Our team focused on sites that presented themselves as Singapore-based, as they could be used by threat actors, either for HICs targeting Singaporeans or for information operations appearing to represent the views of Singaporeans. Both of these pose national security concerns. During sensitive occasions like an election campaign or a dispute with a foreign government, a threat actor could use its nefarious network to influence Singaporeans with disinformation or propaganda, potentially swaying sentiments and opinions.

RSIS' study did not detect any use of networks and sites in HICs against Singapore. However, such networks and sites are like stores of digital ammunition that can be used when the time is right. Previous reports of alleged Russian and Iranian information operations, "Doppelganger" and "Endless Mayfly", respectively, suggest that inauthentic social media accounts would be the means of launching inauthentic news sites to the public.

Countermeasures Needed

Since reports by Mandiant, Citizen Lab, and the South Korean intelligence agency have pointed to the use of inauthentic websites in foreign influence campaigns around the world, the Singapore Government is prudent in restricting them before they can be used to launch HICs against Singapore.

Hence, on 22 October, MHA and IMDA issued directions under Section 16 of the Broadcasting Act 1994 to Internet service providers to disable access to ten inauthentic websites for users in Singapore. Other laws, like the Foreign Interference Countermeasures Act, which presently do not cover such scenarios, might need to be updated.

Besides legislation, enhancing public awareness about the potential of inauthentic websites being used in HICs is also crucial. For instance, there is a need to instil greater awareness of the deceptive goals and tactics used in seemingly benign news on entertainment and lifestyle. This objective can be incorporated into existing digital and information literacy initiatives. Continued efforts in this area – such as the Source, Understand, Research, and Evaluate (S.U.R.E) campaign by the National Library Board – can further nurture the information literacy skills of Singapore netizens.

As an open, diverse and digitally connected society, Singapore is vulnerable to foreign interference through online HICs. As the tactics of foreign threat actors continue to evolve, we need to be vigilant and circumspective about online sources of news or information, especially those that portray themselves as originating from Singapore.

Benjamin Ang is a Senior Fellow and Head of the Centre of Excellence for National Security (CENS) at S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University, Singapore. He is also the Head of Digital Impact Research at RSIS and leads the Future Issues in Technology programme. Dymples Leong is an Associate Research Fellow at CENS.