RSIS COMMENTARY

29 July 2025

As Cyber Threats Grow, Singapore Walks a Careful Line on Identifying State Actors

Muhammad Faizal Abdul Rahman

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

Ponder the Improbable since 1996

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

RSIS COMMENTARY

www.rsis.edu.sg No. 165 – 29 July 2025

As Cyber Threats Grow, Singapore Walks a Careful Line on Identifying State Actors

By Muhammad Faizal Abdul Rahman

SYNOPSIS

As Singapore confronts increasingly sophisticated cyber threats, it continues to take a cautious approach in attributing blame when identifying state actors.

COMMENTARY

The recent disclosure that a cyber threat group, identified as UNC3886, was attacking critical infrastructure in Singapore took many by surprise.

The announcement was made by Coordinating Minister for National Security and Minister for Home Affairs K. Shanmugam during a speech at the 10th anniversary of the country's Cyber Security Agency (CSA) last Friday (18 July). He warned that Singapore was actively dealing with a "highly sophisticated threat actor" capable of conducting espionage and causing "major disruption to Singapore and Singaporeans".

Google-owned cybersecurity company Mandiant has described UNC3886 as a group with a China nexus. Understandably, the Chinese embassy in Singapore was dissatisfied that UNC3886 was described as being linked to China.

One question that may intrigue readers more is why the minister did not link UNC3886 to a particular country. Was this a perfunctory attempt to publicly attribute a cyber threat, or was it a policy decision based on careful strategic calculations?

In his announcement, it was apparent that Shanmugam deliberately focused on only naming the threat group, rather than directly pointing to any country. When he was asked the following day about UNC3886's alleged links to China, he said this was "speculative".

"What Mandiant does is what Mandiant does ... Who they (UNC3886) are linked to and how they operate is not something I want to go into," he said.

Technical vs. Political Attribution

Past cases suggest that when it comes to cyberattacks, Singapore prefers technical attribution over political attribution. The former is based on forensic evidence of tactics, while the latter is based on intelligence.

Without direct state attribution, it is often the media and analysts who examine potential links and broader implications as part of their analysis and reporting. For example, when Singapore telecommunications company Singtel disclosed a malware attack in November 2024, it was a Bloomberg report that attributed it to Volt Typhoon, a group allegedly sponsored by China.

Similarly, when Singapore blocked roughly 100 social media accounts for circulating disinformation in July 2024, including those linked to a right-wing group created by former Donald Trump adviser Steve Bannon, it made no mention of the United States.

During peacetime, technical attribution offers a more pragmatic way to deter cyber threats. Cyberspace is a complex environment, and non-state threat groups, which may or may not act on the behest of a state, are the dominant actors there. This method allows authorities to expose threat groups without directly shaming the country from which they may be operating.

Arguably, not shaming the country where the threat group operates from could risk emboldening future attacks and invite scrutiny from security partners who expect transparency. More importantly, it may make public education about the seriousness of cyber threats more challenging. The public may not understand the full context, for example, of the motivation or geopolitical implications of an attack.

Why Naming Without Shaming

While Singapore avoids attributing cyber threats to specific states, naming and shaming is the preferred approach for many Western countries and some of their Asian allies when it comes to China, particularly those that view it as a preeminent threat.

For countries not directly involved in adversarial relations or those that pursue a foreign policy of non-alignment, it may be more prudent to deter cyber threats without exacerbating geopolitical animosity. The cost of escalation may be too high a risk to bear. Moreover, it remains debatable whether naming and shaming helps to curb cyber threats in a meaningful way.

In Singapore’s context, there could also be other plausible strategic considerations.

First, Singapore is a cosmopolitan country comprising locally born citizens, naturalised citizens and foreigners. Social cohesion is the glue that keeps its people together and maintains communal harmony. Publicly identifying another country as a threat carries the risk of fuelling racism and xenophobia. For example, in 2021, the fear that the

Singapore-India Comprehensive Economic Cooperation Agreement (CECA) posed a threat to the livelihood of Singapore citizens raised the ugly head of xenophobia.

Second, there is an observable trend in which Western cybersecurity companies often attribute cyber threat groups to China following incidents involving Western digital networks. Even if there is forensic evidence to link these groups to China, these companies often hold contracts with the US government, creating both commercial and political incentives to focus blame on China. If Singapore is seen as endorsing these companies' attributions, it risks making the impression that Singapore has shifted its foreign policy of non-alignment and is siding with the US in the strategic rivalry with China, which involves cyber contestation.

Third, while Singapore and China may have differing views on certain issues, both countries at the political level are keen to deepen their bilateral relations. During an official visit to Beijing in September 2024, Singapore Foreign Affairs Minister Vivian Balakrishnan described Singapore-China relations as a “very bright spot” in a more volatile and less predictable world. Such a world is even less black and white, and similar to dealing with the US tariff threat, countries must find a balance between resisting compulsion and promoting cooperation.

It is prudent not to let one issue define the overall state of bilateral relations.

Furthermore, Singapore is a member of the Association of Southeast Asian Nations (ASEAN), and China is a dialogue partner of ASEAN. One essential area where ASEAN and China are cooperating is the ASEAN-China Free Trade Area (ACFTA) 3.0 signed in October 2025, aimed at building economic resilience. ASEAN countries, therefore, need to consider both national and regional interests.

In the same vein, the overall state of bilateral relations, as well as factors such as motivation, impact of attack, and international law, would determine how Singapore responds to cyber threats originating from other countries.

The world is witnessing a growing militarisation of cyberspace where countries in the West, the Middle East and Asia are developing military cyber capabilities. Some may be more willing to conduct offensive cyber operations if their interests with Singapore diverge.

When Naming Might Be Necessary

However, these considerations do not necessarily preclude non-aligned countries like Singapore from naming and shaming any country as a cyber threat actor should the situation justifies it.

A careful examination of what constitutes Singapore’s most vital national interests may provide insights into how and when such a shift in posture might occur.

Plausible scenarios could include external military threats operating in both physical and cyberspace domains, as well as a cyberattack that is not for espionage purposes but creates a disruptive impact that endangers the lives of people in Singapore. For example, imagine a scenario where Singapore faces military coercion and

concurrently a cyberattack by a state-linked threat actor that shuts down the digital infrastructure and electrical systems of hospitals nationwide, resulting in deaths.

These are extreme scenarios that, hopefully, Singapore will never have to deal with, but must prepare for in the unlikely event that they occur.

Muhammad Faizal Abdul Rahman is a Research Fellow (Regional Security Architecture Programme) with the Institute of Defence and Strategic Studies (IDSS) at the S. Rajaratnam School of International Studies (RSIS) at Nanyang Technological University. *This commentary was originally published on CNA on 25 July 2025. It is published here with permission.*

S. Rajaratnam School of International Studies, NTU Singapore
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798

Please share this publication with your friends. They can subscribe to RSIS publications by scanning the QR Code below.