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

RSIS COMMENTARY

www.rsis.edu.sg No. 038 – 3 March 2021

SolarWinds & Cyber Diplomacy: The Missing Piece

By Eugene EG Tan

SYNOPSIS

Relying solely on a domestic response will not end the cycle of global cyber threats. A concerted effort to build capacity, confidence, and rules of the road may bring consequences to states who choose to continue sponsoring hostile activity.

COMMENTARY

IT IS now evident that while the SolarWinds breach affected many government agencies in the United States, and potentially other users of its Orion software like Singapore, the operation has reportedly remained an act of espionage – something most states if not all do in one form or another.

In a statement to the Singapore Parliament on 2 February 2021, Minister for Communications and Information S Iswaran announced that there has been "no indication" that the country's critical information infrastructure and government systems have been adversely affected by the breach. He recognised that breaches like SolarWinds demonstrate how these cyber threats are first, global in nature; second, will happen again; and, third, are difficult to prevent, and called upon all users and operators to be vigilant in tackling cyber threats.

Domestic Responses

The breadth of the breach has however led to some observers to bay for blood, with some calling it an act of war and others to retaliate in a visible fashion. However, while such an act harms national security, retaliatory action for espionage activity may not be acceptable under international law.

Espionage is, to all intents and purposes, not prohibited under international law, which

makes any international response to acts of espionage illegitimate. States are however free to punish these acts based on their respective national laws. Responses to cyber threats that fall under the threshold of international law can thus be separated on two levels: the domestic and the international levels.

Exhorting domestic actors to prepare for future cyberattacks and to remain vigilant makes for good domestic policy and will not antagonise other states. But these actions are limited because they do not fundamentally change the behaviour and motivations of state-sponsored threat actors.

It is therefore interesting that Singapore has chosen to strengthen its domestic response rather than to build an international or regional consensus on the SolarWinds breach. Singapore has not chosen to punish or push its own attribution of the state actors behind the SolarWinds breach, but has instead chosen to focus on its own protocols and taken steps to strengthen its own cybersecurity processes.

Taking steps to improve the resilience and robustness of domestic systems will make it harder for malicious actors to access critical systems and potentially decrease the benefit they derive from compromising these systems. But these steps on their own will not prevent future cyber threats from external sources.

Expanding Role of Cyber Diplomacy

As cyber threats are becoming more global in nature, there is much more to be considered in an international response to a cyber threat like SolarWinds. As a small state that seeks to be a friend to all, escalating any cyber incident will not benefit Singapore's national security posture. This does not mean, however, that state-sponsored cyber incidents should remain unaddressed and without consequence to the offending party.

Small states like Singapore should therefore consider and review their cyber diplomacy efforts to combat cyber threats. These efforts include building norms of responsible state behaviour, capacity building, and confidence building, which are all pillars of contained in the 2015 UNGGE consensus report.

Pillar 1: Norms for Responsible State behaviour

Singapore firmly believes that having stronger rules of the road will help define acceptable state behaviour in cyberspace. Singapore has been plugging into the different international conversations at the United Nations like the Open-ended Working Group (OEWG) and the Group of Governmental Experts (UNGGE) to advance discussions on the rules of responsible state behaviour in cyberspace.

Regionally, Singapore has also been pushing for progress on the adoption and the operationalisation of 11 norms of responsible state behaviour. Additionally, a mechanism for cyber cooperation among ASEAN member states was also proposed at the 2018 Singapore International Cyber Week.

When fully operationalised, the combination of the normative framework and

cooperation mechanism can lead to a coordinated response that carries the full force of all ASEAN member states.

Pillar 2: Capacity Building

Singapore, through its ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE), has also been actively building technical, policy, and legal capacity among ASEAN member states.

The benefit of the centre is two-fold: first, it enables states to discharge their obligations and responsibilities in cyberspace such as due diligence; and, second, it builds the trust and assurance among partners in the region. This will ensure that our regional and international partners can be trusted to have the expertise to tackle any cyber breach in the future.

Pillar 3: Cyber Confidence Building Measures

What Singapore needs to improve on in its cyber diplomacy efforts, however, is the third pillar of the 2015 UNGGE report – cyber confidence building measures. Cyber Confidence Building measures are even more important in times of geopolitical tension, and can be done by increasing interstate cooperation to improve the transparency, predictability, and stability of cyberspace.

Confidence building measures recommended by the 2015 UNGGE such as cooperation on cybercrime, the creation of a points of contact directory, and a mechanism for threat information exchanges among states, have however been given the short shrift by states. It would make sense for states to build trust among stakeholders – both public and private.

It is a given that cyber threats will increase and it is unclear where the next cyber threat will come from. It would therefore make sense for Singapore to build cooperation mechanisms like an information sharing network to build confidence among stakeholders and to stymie any potential cyber threat actor.

In a sense, the reporting of the SolarWinds breach by the US government was in fact an act of transparency and a confidence building measure through the sharing of information of the threat vector.

In short, while it is important for small states like Singapore to strengthen its domestic tools and responses against global cyber threats like Solarwinds, they can also find ways to cooperate with each other through the various cyber diplomacy tools for better cybersecurity.

Any confidence building measures, capacity building, and norm implementation effort however requires the willingness of all states and stakeholders to be fully effective; more should be done to bolster the diplomatic effort to dispel the notion that malicious actions in cyberspace have no consequences.

Eugene EG Tan is Associate Research Fellow at the Centre of Excellence for National Security (CENS), a constituent unit of the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore.

Nanyang Technological University
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798
Tel: +65 6790 6982 | Fax: +65 6794 0617 | www.rsis.edu.sg