Australia under cyber attack : dissecting Canberra’s response

Tan, Eugene E. Guang

2020

Tan, E. E. G. (2020). Australia under cyber attack : dissecting Canberra’s response. (RSIS Commentaries, No. 143). RSIS Commentaries. Singapore: Nanyang Technological University.

https://hdl.handle.net/10356/143826

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

RSIS COMMENTARY

www.rsis.edu.sg No. 143 – 15 July 2020

Australia Under Cyber Attack: Dissecting Canberra's Response

By Eugene EG Tan

SYNOPSIS

Attributing cyber attacks to state-sponsored actors is a delicate balancing act that requires strategic and political thinking. States may or may not choose to name the offending state based on their own national interests. What is more important is how states should improve their capabilities to actively deter malicious actors.

COMMENTARY

ON 19 JUNE 2020, Australia publicly announced that it was a victim of state-based cyber attacks. This assessment was based on the "scale and nature of the targeting". According to Australian Prime Minister Morrison, the malicious activity was targeted at a broad range of organisations across Australia, including government, industry, political organisations, education, essential service providers, and operators of critical infrastructure.

The Australian government did not disclose the identity of the attacker or the objectives of the attackers. Morrison particularly stressed that there were no large scale data breaches of private information, and that the announcement was a public call to improve capabilities in face of aggression caused by states. This raises questions of why did the Australian government feel the need to attribute a cyber attack when there was little harm done.

Cyber Conflict – More of the Same?

To understand this better, it should be remembered that cyber conflicts among states are still largely driven by geo-political and political considerations, and should not be seen as separate from other kinds of conflict or political objectives.

The increasing use of cyber operations can offer new ways to test the robustness of a state's defences – in this case networks, but they are usually part of great power competition or the hierarchy of states in the international system. States sponsor malicious actors to degrade networks, disrupt services and collect information through espionage activity.

It is therefore unsurprising that prominent think tanks in Australia have suggested with a high level of confidence that China, given its recent tensions with Australia, was behind the attacks. But this may not be the case because think tanks may not have all the information that the government has, and do not represent government positions.

Attribution – a Signalling Device

Publicly attributing a cyber attack is one of the many responses available to states, but states may choose to withhold the identity of the perpetrator.

The Australian government's approach may have more nuanced national security considerations. Australia had previously, with the United Kingdom, accused Russia of cyber attacks aimed at destabilising democracies in 2018. Unfortunately, pointing the finger at Russia had little effect in reducing cyber attacks but instead increased hostility and mistrust of Russia.

By not naming the state actor, victim states can signal in two main ways: first, signal in the first instance to the aggressor their capability in discovering and resolving a cyber operation; and second, that these activities should cease. Should the 'signal' not be heeded, the victim state can then proceed to escalate the attribution by naming who the perpetrator is.

This is not dissimilar to Singapore's response to the SingHealth cyberattack in 2018. Then, Singapore took the same tack of attributing the attack to a state-sponsored actor while not naming the perpetrator. As a small state, Singapore seeks to maintain good relationships with all states, meaning these relationships should not be jeopardised. The act of not naming a state allowed the offending state some leeway to back away to de-escalate.

Calculated Responses to Cyberattacks

Responding to a cyber attack is tricky and may have many spill-over effects that may affect the strategic and political calculation and interests of states. What states can do well is to consider all possible information and options before responding.

Small states like Singapore need to be careful in any response because a disproportionate response to a cyberattack may results in escalation by the attacker. This could be potentially catastrophic given the vulnerability of the state's economy, infrastructure, and physical size.

When people call for retaliation for cyber attacks they miss the point on how states can react to a cyber attack. Small states have serious limitations in their credibility and ability to punish state-sponsored perpetrators, especially from much larger states. The realities of small states' physical vulnerabilities cannot be discounted.

Hypothetically, if a large state carried out a cyber attack, small states would be hard pressed to impose economic sanctions, or to show military or cyber force. At best, small states could use diplomatic back-channels to signal their displeasure.

Improving Domestic Responses to Cyber Operations

It is unfortunate that most reports on Morrison's remarks circle around the whodunit element of attribution. While reacting adversely to a cyber-incident may be an understandable and natural reaction, Morrison's remarks were also in part to help the public understand that part of the response required domestic attention, and the Australian government was actively trying to defend against these malicious actors.

Domestic responses such as building cyber and societal resilience are also important for states to combat the effects of cyber operations. By reducing the time that systems are disrupted by developing continuity of business plans, the effects that an adversary seeks can be mitigated.

The payoffs for a successful cyber attack in the physical realm often manifest itself in either the physical destruction of infrastructure or the psychological disruption in the minds of the residents of the state. However, if attackers cannot realise these payoffs, then there may be less motivation for an attacker to carry out a cyber attack because the level of success is low.

Attribution of an attack should therefore only form part of the response of the state, and should not be considered the first response to a cyber incident. Instead, the increased awareness of the targets, motives and *modus operandi* of state-sponsored malicious actors may guide states to create a more robust response mechanism that is effective to deter and communicate costs to an aggressor state.

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