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

RSIS COMMENTARY

www.rsis.edu.sg No. 001 – 4 January 2021

"Offensive Cyber" and Espionage: Dirty Secrets No One Talks About

By Shashi Jayakumar

SYNOPSIS

A combination of one of the oldest professions – espionage – with one of the newer ones – cyber hacking – has led to hyperbole and threats of kinetic escalation. But is all this talk really warranted? What will the real fallout be?

COMMENTARY

RECENT REVELATIONS concerning the compromise of SolarWinds' Orion network management platform through the backdoor insertion of malicious code are noteworthy in part because of the soul-searching that followed within the US political and security commentary. Many US government agencies were amongst its victims.

The reactions stem from three factors. The first is sheer embarrassment. The hacking appears to have been done by the SVR – the Russian foreign intelligence service. Its exposure is at a sensitive moment in US history – and with Russia in the security crosshairs due to earlier episodes such as electoral interference. Secondly, this was not a run-of-the -mill exploit. This was a sophisticated "supply chain" attack aimed compromising a trusted tool which downstream clients would assume is safe.

Distractions on Two Fronts?

The third factor is a conceptual one, and has to do with the mistaken notion that what happened amounted to OPE (operational preparation of the environment), or preparation for destructive attacks. The separating line between OPE and intelligence collection in the domain cyber can be fluid; there is little evidence too that there was an attempt to convert this espionage operation into evidence of a destructive attack.

The somewhat bellicose talk of kinetic retaliation has proved something of a distraction

from two issues. The first is a perceptual one. From the point of view of US' adversaries – and even some allies – the US has been engaged in the same game for some considerable amount of time.

The Snowden revelations have shown this, and there has also been more recently some light thrown on spying through technical means, sometimes in concert with select trusted partners, against other nations (including friendly ones), in the form of the Crypto AG scandal.

The second distraction may be one with internal ramifications. What should not be forgotten from the Solarwinds episode is where the real remediation efforts lie. There should be a comprehensive breach notification law (which currently is only addressed at the state level) for the private sector in the US.

And crucially, the incoming Biden administration needs to initiate a comprehensive cross-governmental effort (including the Department of Defence vendors, and the Department of Homeland Security) to address software and hardware vulnerability from vendors. These things are difficult to do, but necessary, and may in fact be the real learning lessons that should be heeded.

Retaliation and Deterrence

The US has the tools in its cyber arsenal to retaliate as well as the doctrinal blueprint to do so, having evolved offensive doctrine that provides a conceptual and operational framework to respond to cyberattacks. The culmination of this thinking came in the form of two seminal documents in 2018:

The first is the White House's National Cyber Strategy (NCS) which warns of developing "swift and transparent consequences" "to deter future bad behaviour"; the second is the DoD's own Cyber Strategy which makes pointed mention of the concept "defending forward", or halting malicious cyber activity at its source, which includes, it must be presumed, extraterritorial cyber operations.

Imposing costs on the adversary, and resetting adversary expectations in cyberspace, have therefore now become essential parts of US offensive cyber doctrine. Core to this even in times of peace is activity in adversary networks.

But activity and interdiction also take place in "grey zones" (as defined by the US), which might be networks of neutral states or even states allied with the party initiating action. This is a grey area in international law, with very little discussion on what happens when states seek to transit through nodes located elsewhere, or interdict others, when the adversary in question is another state.

Solarwinds, Supply Chain Compromise & No Red Lines?

A supply chain compromise is one matter. But nations engaging in persistent forward defence – and here one must assume that several nations think similar as the US ─ may choose to up the ante especially if engaging in retaliatory action.

They might for example put in place assets that could compromise or even cause

damage to critical infrastructure. The line between reconnoitering and the emplacing of these assets (as a preparatory to a cyber attack), is recognised to be grey area by many experts; and for some nations, this may cross the “use of force threshold” justifying an armed response, although there is no international consensus on this.

There is, in short, the risk of miscalculation in a realm where there is no accepted codification of red lines.

As some respected commentators have observed, it is unclear what aspect of international law would have been contravened by the Solarwinds espionage incident. The norms agreed at the 2015 UN GGE (Group of Governmental Experts) also do not cover espionage activities.

Officials from major cyber powers have spoken generally about international law in cyberspace but have not been precise when it comes to how international law interacts with their right to defend themselves.

This criticism is not specific to the US: other major cyber powers, while agreeing in general terms that international law applies in cyberspace, are chary of contributing to discussions on enforcement mechanisms.

Norms do matter but not that much. The discussions themselves must and will of course continue, but it is extremely unlikely that as it stands they will prevent cycles of escalatory retaliation ─ or espionage when it serves the interest of the state. This is illustrated in the willingness of states (or hackers working at the behest of a state) to attempt cyber-enabled espionage to discern the extent of the COVID outbreak in other countries and the actions being taken against the virus.

Southeast Asia: Friends in Need?

Cyber discourse is not as well developed in Southeast Asia as it is in the West. Nations in the region have shown signs of participating more actively in discussions on advancing responsible state behaviour on cyberspace.

But when it comes to thorny issues such as attribution of cyberattacks, and taking a stance on whether hostile cyber operations that are not physically destructive (but might affect critical infrastructure, or even undermine governments) can constitute a use of force, no firm positions are taken.

Singapore and Southeast Asian nations should prepare for scenarios that might see intensified conflict within the cyber arena by the major powers -- conflict that might test existing, ambiguous, positions. Nations may come under pressure, for example, to attribute cyberattacks.

Singapore has suffered major hacks before – with the most serious, the IHiS/SingHealth breach, almost certainly the work of state-linked actors, although following the usual practice, no specific official attribution was made.

Separately, APT (Advanced Persistent Threat) groups thought to emanate from the region have targeted Singapore-based firms, a case in point being APT 32, or Ocean

Lotus. The identification of APT32 with Vietnam has recently been confirmed by Facebook in its own investigations.

Besides calling out aggressors (or being pressured to do so), another possible scenario might see countries in the region facing situations where major powers seek grey zone cooperation on the denial of space for others to operate, perhaps in the context of an offensive cyber campaign.

These would be difficult situations to be placed in, and they may, or may not, transpire. They may in fact already be happening. Their very possibility refreshes the seemingly tired adage that there are no permanent friends in statecraft.

Especially not in cyber.

Dr Shashi Jayakumar is Head of the Centre of Excellence for National Security and Executive Coordinator for Future Issues and Technology at 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