Thayer Consultancy
ABN # 65 648 097 123

Background Brief:

Vietnam and Cyber Security

Carlyle A. Thayer

February 20, 2021

We are preparing a report on Vietnam's rise as a power in cyberspace, and request your insights into the following issues:

Q1. What is the status of the implementing guidelines to Vietnam's 2018 Law on Cybersecurity?

ANSWERS: The draft guidelines for the Law on Cybersecurity have not been released according to the public record. There are two "recent" reports both dated last year.

On 23 April 2020, a spokesperson the Ministry of Foreign Affairs, was quoted as saying that the National Assembly "is finalising guiding documents on the law."

The second reference is dated 29 May 2020. Bui Van Nam, the Deputy Minister of Public Security, called on public security units and agencies to advise authorities at all levels to "urgently advise the Government to issue a decree guiding the implementation of the Law on Cybersecurity."

Q2. Considering Vietnam's activity online over the last few years, do you assess that Vietnam deserves to be considered – like China, N. Korea or Iran – among the most powerful and aggressive state actors in cyberspace?

ANSWERS: While the OceanLotus Group (also known as Advanced Persistent Threat 32 or APT32), based in Vietnam, has been active for at least nine years, and by all accounts has become more sophisticated, including the development of it own custom-built tools and software, it does not operate with the same scope and depth as state hackers in China, North Korea and Iran.

According to a FireEye analyst in 2016, APT32 was capable of conducting "multiple campaigns simultaneously [and had] the resources and capabilities to execute devastating large-scale network attacks…"

The OceanLotus Group has demonstrated it has the resources and capacity to pursue targets for spear phishing for a prolonged period. In 2017, the director of FireEye revealed that APT32 spent at least three years targeting "foreign corporations with a vested interest in Vietnam's manufacturing, consumer product and hospitality sectors" in Asia, Germany and the United States.

Three types of groups have been identified as APT32 targets: (1) Vietnamese dissidents including civil society and human rights activists and foreign journalists

living in Vietnam and abroad, and non-governmental organisations, (2) commercial enterprises in Germany, the Philippines, Vietnam, and the United States (agriculture, hospitality, hospitals, information technology, mobile services and retail outlets), and foreign car manufactures (BMW, Hyundai and Toyota), and (3) governments (Cambodia, China, Laos) and multilateral institutions (ASEAN).

In 2019, Volexity reported that OceanLotus conducted a sophisticated mass digital surveillance campaign beginning in 2017 that has continued to evolve. OceanLotus set up and operated for several years multiple activist news and anti-corruption websites. These fake websites enabled OceanLotus "to have full control over the tracking of and attacks against website visitors."

In December 2020, two senior officials at Facebook concluded that the latest activities conducted by APT32 have " the hallmarks of a well-resourced and persistent operation focusing on many targets at once, while obfuscating their origin."

Most recently in 2020, OceanLotus has been implicated in hacking attacks on China's Ministry of Emergency Management, the Wuhan Municipal offices and Cambodian government agencies.

Q3. What do you think the future holds for Vietnam's online security?

ANSWERS: In March 2020, *The Journal of Engineering* reported that Viettel Cyber Security Company, a member of the military's Viettel Group, stood up a Managed Security Operation Center with a staff of 200 to provide "service on a global scale capable of detecting, analyzing, responding, preventing and investigating traceability of information security incidents and ensuring security for IT systems in Vietnam."

The journal noted that Viettel Cyber Security Company "is the first information security company in Vietnam to have a complete security ecosystem researched and developed by Viettel's security experts." Nguyen Son Hai, the Director of the Viettel Cyber Security Company, was quoted as saying he wanted his company "to become the largest cyber security provider in Vietnam" to large enterprises, organisations, and critical national security infrastructure.

The recently concluded thirteenth national congress of the Vietnam Communist Party set a goal of promoting the Fourth Industrial Revolution, including e-commerce and the digital economy, in coming decades. This will raise the priority for providing online security for commercial and government internet users.

According to Nguyen Trong Duong, Deputy Director General of the Information Security Authority of the Ministry of Information and Communications, speaking in February 2020, there was a 300 percent rise in data breaches involving domestic commercial enterprises in 2019 over the previous year. The Vietnam Cybersecurity Emergency Response Team reported that there was a 104 percent rise in hacking of domestic information systems over the same period.

In addition, the Information Security Authority reported that 49.4 per cent of Vietnam's financial institutions have set up a specialised unit to ensure information security. But only 9.2 per cent of these units could construct their own security monitoring systems. Only one-quarter of Vietnam's financial institutions are able to

detect malicious attacks, while the remaining seventy-five percent can be attacked without detection.

It is inescapable that the Ministry of Public Security and other government agencies, will avail themselves of evolving technology to step up surveillance of the internet to combat criminal activity directed against Vietnam's financial and commercial enterprises. It is highly likely that relevant technologies will be harnessed to conduct surveillance on the general population to target human rights and civil society activists.

Suggested citation: Carlyle A. Thayer, "Vietnam and Cyber Security," *Thayer Consultancy Background Brief*, February 20, 2021. All background briefs are posted on Scribd.com (search for Thayer). To remove yourself from the mailing list type, UNSUBSCRIBE in the Subject heading and hit the Reply key.