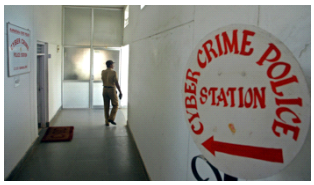
New players join race for offensive cyber abilities

Monday, August 20, 2018

Brazil, South Africa, India and Vietnam are investing in developing both defensive and offensive cyber capabilities



A Cybercrime Police Station in India
(Reuters/Jagadeesh Nv)

The proliferation of offensive cyber capabilities continues beyond the headline-making actors. Many states are trying to capitalise on this relatively new domain of competition, including Brazil, South Africa, India and Vietnam.

What next

Brazil, India and Vietnam are all consolidating their cyber capabilities into new command structures, but South Africa's effort to do the same is being impeded by budgetary constraints. States and businesses, particularly those operating in strategically relevant sectors, should expect cyber risks to become acute as offensive capabilities come online in an ever-growing number of countries.

Subsidiary Impacts

- Businesses investing or partnering with entities in Vietnam face a particularly high risk of being targeted by state-linked actors.
- Corporate investment in cybersecurity will rise in nearly all developing countries, albeit slowly and unevenly.
- Theft of digital personal data will fuel political pressure for proactive cybersecurity strategies.

Analysis

Cyber capabilities are continuing to proliferate beyond the more well-known cyber powers -- the United States (see RUSSIA: US charges designed to prove hacking - July 27, 2018), Russia, China, United Kingdom, Israel, France, North Korea and Iran (see IRAN: Tehran may prioritise cyber espionage - July 11, 2018).

New players include Brazil, South Africa, India and Vietnam, but their efforts tend to be particularly underreported in the mainstream press.

Brazil

In an effort to prioritise cybersecurity, Brazil formed the Center for Cyber Defense in 2010, whose capabilities were built up for and tested in two major events -- the 2014 football world cup and the 2016 Olympics. In 2016, the government further integrated its cyber capabilities from various parts of the armed forces into a 300-person-strong joint operational command called Cyber Defense Command.

Little is known about Brazil's offensive capabilities, except that the armed and intelligence services oversee them.

However, one significant unattributed advanced persistent threat (APT) -- a term that usually refers to state-linked offensive cyber actors or to sophisticated cyber criminal networks -- focused on espionage has been operating in South America since at least 2010, under the alias 'El Machete'.

Most of its victims are located in countries neighbouring Brazil: Ecuador, Venezuela, Peru, Bolivia, Argentina and Colombia.

Further targets have been identified in the Dominican Republic, Canada, Cuba, the United Kingdom, Germany, Guatemala, Mexico, Nicaragua, Russia, Ukraine and the United States.

They have included security-relevant organisations, such as military and intelligence services,

embassies and utility providers. This would be consistent with the use of cyber capabilities for foreign intelligence purposes and would match Brazilian foreign and security policy interests.

While Brazilian intelligence capabilities have been abused for domestic political gains in the past, no indications exist of their use for direct commercial gain.

South Africa

South Africa has suffered various large data breaches in the last twelve months. The most notorious incident reportedly involved the breach of personal data of over 30 million South Africans from a server linked to a Pretoria-based real estate holding company in October 2017.

Such breaches have increased pressure on the government, as well the private sector, to improve cybersecurity.

In particular, the State Security Agency's National Communication Centre (NCC) -- the core cybersecurity agency -- is attempting to upgrade its currently limited signals intelligence capabilities in the area of bulk and targeted interception.

During 2013-15, various media reports based on leaked company documents said that the NCC is a customer of FinFisher, a German cyber surveillance vendor, which among other services, sells interception capabilities.

As part of its cyber strategy, South Africa is also developing offensive capabilities under the National Defence Force's Defence Intelligence Division.

However, funding shortages in the defence department, due to a stagnating economy, have delayed its plans to establish a Cyber Command Centre Headquarters to the April 2019-March 2020 fiscal year.

India

Being home to a large pool of IT talent, India has the technological skills-base to become a major cyber power. Yet the government's approach to cybersecurity has thus far been uncoordinated, with capabilities developed disparately across multiple security agencies, including the intelligence agencies and armed forces.

Differing levels of cyber preparedness have in the past compromised internal and external operations of both the military and civilian security agencies.

A key vulnerability appears to be the use of the same contractors without effective operational coordination.

This weakness was exemplified in 'Operation Hangover', uncovered in 2013, which targeted Norwegian Telenor as well as Pakistani and Chinese entities for national security and corporate espionage purposes and was found to be linked to Indian cyber actors.

India's reorganisation shows a will to upgrade cyber capabilities

The National Technical Research Organisation, led by the National Security Advisor, is likely home to India's most advanced offensive cyber capabilities. It probably also has agreements with other neighbours of China such as Mongolia on technical assistance in traffic interception.

After many years of disjointed initiatives, India earlier this year decided to consolidate its military cyber capabilities in the Defence Cyber Agency. The agency, comprising about 1,000 people from across the armed forces, is a starting point for a future cyber command.

Such capabilities would be deployed for both foreign intelligence and domestic security purposes, and

are likely to be particularly targeted at China, followed by Pakistan.

Since 2013-14, there has been a visible rise in the targeting of Chinese entities by an allegedly India-linked cyber actor aliased 'Dropping Elephant'.

Vietnam

For Vietnam's government, cyber risks stem not only from the poor security of computer networks and digital systems but also from the free sharing of information across digital channels by citizens and residents. Both types of insecurity have been a serious concern for Hanoi since at least 2012 (see SOUTH-EAST ASIA: Cyber risks are rising - August 15, 2018).

In 2017, the military revealed the existence of a 10,000-strong cyber unit known as 'Force 47', tasked with combatting dissenting political views. In early 2018, the government announced the formation of a cyber command, consolidating the efforts across the armed forces.

These do not appear to be new efforts: rather they are administrative bodies stepping out of the shadows.

Cyber security companies have also long tracked an espionage APT known as 'APT32/Ocean Lotus', which has been active since at least 2012 and whose activities appear to advance Vietnamese state security goals.

Domestically, its targets include civil society targets (for example, journalists and human rights organisations) and foreign businesses operating in Vietnam.

> Vietnam appears to be particularly successful at cyber espionage

Abroad, this threat actor has targeted international organisations, governments and strategically relevant private sector entities in Australia, Cambodia, China, Germany, Laos, the Philippines and the United States, and included maritime agencies, maritime infrastructure companies and shipping enterprises, according to the Western cybersecurity firm FireEye.

For example, the firm reports that a European company was targeted "prior to constructing a manufacturing facility in Vietnam".

Therefore, businesses considering investing or partnering with entities in Vietnam carry significant risk of being targeted by this APT actor.