COMMENT

Bolstering defence in cyberspace

CYBER ATTACKS: Need to understand scale of aggression, right response time

LAST year, the discovery of China's alleged hacks into the United States's Office of Personnel Management (OPM) files raised questions on the US legal response to operations in cyberspace. Reuters reported that an estimated 22 million US federal workers were affected by the hacks.

Intelligence gathering belongs in an ambiguous area of international law. The hacks were raised during Chinese President Xi Jinping's meeting with US President Barack Obama during the former's state visit to the US in September last year. In December, the White House finally released a cyber deterrence policy that included an array of possible retributive actions, such as law enforcement, sanctions, defensive cyber operations and, of course, the possibility of using military force.

Though China denied responsibility, the issue raised questions on attribution and the appropriate responses to a cyberattack.

The media-hyped US-China cyber conflict was not the only headline last year. In the beginning of the year, the Shanghai Cooperation Organisation, comprising states such as China, Kazakhstan and Russia, updated an earlier Code of Conduct regarding information and communications technologies that had been presented to the United Nations General Assembly in 2011.

Apart from numerous agreements among states to combat cybercrime and conduct joint research on the technological aspects of cyberspace, the UN's Group of Governmental Experts (GGE) also released a list of norms for conduct in cyberspace, including prohibition against the intentional damage of a state's critical infrastructure or targeting of emergency response systems through cyberattacks; promise of supply chain integrity; and assistance for other nations to investigate cyberattacks and cybercrime launched from their territories.

With last year having played its part to shed light on the darkness of cyberspace, what will this year present?

FIRST, hopefully, an address of Article 51 of the UN charter that grants the right of self-defence to member states in the case of an armed attack. The past GGE on information security meeting ended with a determination of norms. However, the consensus report it issued mentioned the need to look into the codification of international laws regulating the right of self-defence in cyberspace. The legal means of declaring war is important, especially to regulate actions in an operational domain vulnerable to attacks of the least aggression to those on critical infrastructure. In the case of the OPM hacks, the act of espionage was low in aggression, but its infringement on intellectual property and access to information on a large number of individuals drew Obama to place sanctions as an option for retaliation.

The UN charter imposes an obligation on states to maintain peace (Article 39), prohibits threats and uses of force (Article 2(4)) and provides for the right of self-defence (Article 51). Classic *jus in bello* (limitations to the conduct of war) looks at proportionality as a moral compass for retribution.

In an interdependent world, sanctions can have a crippling impact on a nation's economy and political standing. But, the lack of clarification on Article 51 complicates the appropriate responses to acts that can be deemed low in aggression.

Discussion on the applicability of self-defence against attacks in cyberspace has to pursue an understanding of the scale of aggression and appropriate time of response. With the next GGE convening later this year, hopefully, the matter will be addressed.

SECOND, as nations begin war gaming cyber conflicts, perhaps, there will be advancements in the understanding of the limits of cyberwarfare. The cyberattacks that serve as a reference for persistent state-sponsored activities are those that occurred in Iran in 2010 and Estonia in 2007. In Iran, a nuclear facility's functions were halted, while a coordinated attack targeting Estonia's computer systems rendered useless services in the public and private sectors. Since then, war games have served as a test for critical information infrastructure resilience.

However, the outcome of war games can be limited by a virtual belligerent's weak strategic objective and inadequate understanding of operations in the cyber domain.

The recently announced China-Indonesia Joint Cyber War Simulations aim at looking at government responses to cyberattacks on civil infrastructure, with a focus on cybersecurity in national infrastructure development. The joint exercise can facilitate the exchange of information, as well as serve as a step forward towards a proactive culture, especially with objectives that look beyond hardware and software vulnerabilities. War gaming cannot strengthen only system resilience, but must also refine the understanding of national infrastructure, governing operations, as well as domestic and international laws.

THIRD is the expansion and enhancement of interstate relations in regards to cybersecurity.

The saying goes that as the spear becomes sharper, the shield becomes thicker. The gap between actors will widen, divided by technological capacity, knowledge, intent and opportunity. In a bid to demonstrate cyber power, states will develop machines of greater capacity. Thus, what will be increasingly needed is a network of cooperation between developed and developing nations to enable technological and knowledge transfer.

Malaysia's approach to cybersecurity is anchored by the management of information security, with issues such as data leakages and integrity being a priority. At a time when the shape of cyberwar is being formed, threat assessments based on known quantities may not be adequate.

Hopefully, this year moves debates on cybersecurity forward in the country, with concrete actions taken for national interest.

farlina@isis.org.my

The writer is an analyst in the Foreign Policy and Security Studies programme, Institute of Strategic and International Studies, Malaysia

> "...what will be increasingly needed is a **network of cooperation between developed and developing nations** to enable technological and knowledge transfer.

FARLINA SAID