Draft for discussion

Asean must do more to combat military activities in cyberspace

BA HAMZAH[1]

As Asean member states invest more in military capabilities in the cyber space, the need for rules and norms of responsible state behaviour becomes very pressing. To avoid surprise attacks, unintended and accidental encounters by states, proxies, and false flags, for example, Asean states can emulate NATO which has produced a document on international law governing military cyber operations.

The Association of Southeast Asian Nations has been long on promises but short on implementation when it comes to cooperation on cyber security. The Asean member states have been discussing need to combat cyber-attacks and terrorists misuse of the cyberspace since 2006 (Asean Regional Forum, 28 July 2006). More significantly, the Asean Summit at Manila in November 2017 adopted a number of measures to cooperate and prevent cybercrimes. They included need to harmonise laws on cybercrimes and electronic evidence as well as the need to cooperate with Asean Dialogue Partners. There was also commitment to work closely with agencies like ASEANPOL, EUROPOL and the INTERPOL.

There is no shortage of resolutions in Asean calling for cybersecurity cooperation and combatting cybercrimes. But so far, beyond rhetoric there is little real commitment to establish the norms of responsible state behaviour among the ten-member states. At the recent 51st Asean Foreign Ministers meeting at Singapore (August 2018), the Ministers further reaffirmed commitment:

- To formalise an Asean cyber security mechanism to coordinate cyber security.
- To support the eleven voluntary, non-binding norms recommended in the 2015 Report of the United Nations Group of Governmental Experts in the Field of Information and Telecommunications in the context of International Security (UNGGE).
- To focus on regional capacity building in implementing the agreed norms.
- To form the Asean Network Security Action Council (ANSAC) to prepare a proposal paper for "a formal ASEAN cybersecurity coordination mechanism".

The time is now ripe for Asean to seize the opportunity to concretise the paper commitment. Over the years, most notably since 2006, there has been a significant rise in the number of cyber incidents and cyber mercenaries worldwide. The national critical infrastructure—banking systems, water treatment plants, power grids, ports and roads-have become vulnerable to hacking and other forms of cybercrimes. So far, no Asean member has admitted of similar attacks. However, attacks on critical infrastructure have already occurred in Iran, United States, Ukraine and Estonia, among others.

In 2010, the US and Israel intelligence used a malware-the Stuxnet- to partially disable the Iranian nuclear weapon programme. The Stuxnet was the first digital weapon used by a

[1] Lecturer in Strategic Studies, National Defence University, Malaysia. Prepared for discussion at Thailand NADI Meeting, Chiang Mai,25-28 February 2019.
E-mail: bahamzah8@hotmail.com

nation-state to intentionally cause "physical damage to an adversary's industrial control system."

While blaming Israel, North Korea, China, Iran and Russia for cybercrimes, the US is no saint. According to the *Guardian* "more than 45,000 attacks recorded in ninety- nine countries including the UK, Russia, India and China in 2017 may have originated with the "theft" of 'cyber weapons' from the US National Security Agency".

In the past, cyber-attacks have rarely created political risks. They now do as national assets are digitised, easy targets to cyber mercenaries. Security in the digital domain becomes more complex when governments, state-owned companies and proxies also use the cyber space for coercive power projection purposes, where the lines between offense and defence are blurred.

In 2016, the US Cyber Command awarded one contract worth US$460 million to "six private companies to undertake offensive cyber operations." In the ***Worldwide Threat Assessment*** (2019), the CIA posits that "the potential for surprise in the cyber realm will increase in the next year and beyond as billions more digital devices are connected—with relatively little built-in security—and both nation states and malign actors become more emboldened and better equipped in the use of increasingly widespread cyber toolkits."

The WTA reckons the US will be a major target of cyber operations. To deter the threat, the US has empowered the Cyber Command to launch cyber-attacks on the guilty foreign nations and their proxies. According to the WTA, some forty countries have the capability to mount cyber-attacks, a fourfold increase since 2011.

David Sanger revealed in ***The Perfect Weapon*** that, since 2015, the US military has armed its Cyber Command with an offensive virus capable of dismantling Iran. Operation *Zeus Nitro* was devised to disable "Iran's air defences, communications systems and crucial parts of its power grid" as back-up to the Stuxnet.

The biggest challenge in managing the security in the cyber domain is the absence of internationally recognised rules similar to the Geneva Convention of 1949. The UNGGE was tasked in 2016/2017 session of the UN General Assembly with the study of "existing and potential threats in the sphere of information security" and measures to address them, including "norms, rules, and principles of responsible behaviour of states, confidence-building measures, and capacity-building." Without support from the member states, the UNGEE process has reached a dead end. Reason: many states are not willing to surrender sovereign right over cyber security to the United Nations.

Under the current UN Charter, any state can use force to retaliate against an aggression by invoking Article 51 of the UN Charter: the "inherent right of self- defence". Suppose Saudi Arabia were to classify a cyber- attack from a foreign source (e.g., Iran) on one of its critical assets as an act of aggression and take reprisal measures in self-defence, would it not clandestinely start a new war in the Middle East? The tit-for-tat dynamics is precisely why David Sanger warns cyberweapons can be so effective for "states of all sizes" to exercise coercive influence cheaply "without starting a shooting war."

The absence of international law regulating military activities in cyberspace, which accounts for the inherent right of self-defence and the law of state responsibility, plus the authorised countermeasures under the doctrine of self-help can be fatal to the long-held concept of sovereignty. Hence, rules preventing aggression and intervention in the internal affairs of sovereign states via the cyber space are critical to maintain international peace and order.

Whether in the cyber or terrestrial domain, an invasion is still invasion. Not only we cannot see the movement of troops across borders, we only learn of the identity of the perpetrators post incidence. Although cyber weapons have upended the traditional definition of force under international law, such activities remain illegal.

The problems of anonymity, secrecy and attribution are peculiar to cyberwarfare. Nation-states can hide their cyber operations by outsourcing them to third parties. Often, the effect of cyber operations hardly creates any physical damage unlike in a typical

conventional military operation. As Asean member states invest more in military capabilities in cyberspace, the need for rules becomes very pressing.

To avoid surprise attacks, unintended and accidental encounters by states, proxies, and false flags, for example, the Asean member states can emulate the North Atlantic Treaty Organisation, which produced the Tallinn Manual 2.0 on the international law applicable to cyber operations. Although these rules are not binding, they provide a framework for cooperation and confidence building.

I call on the Asean Defence Ministers Meeting, to jointly develop the rules for military operations in the cyber domain as a matter of urgency.