NEW STRAITS TIMES

15 April 2014|

Vital to beef up cyber security

ACT NOW: Asean must lay an intellectual foundation and framework to preserve security in a borderless domain

Elina Noor is ISIS Malaysia assistant director, foreign policy and security studies

LAST week, the world got a feel for what a Heartbleed on the World Wide Web is like. The encryption bug -- referenced unromantically in actual fact as CVE-2014-0160 -- compromises security and privacy of communication on the Internet so that sensitive information such as usernames and passwords are vulnerable to theft. Estimates of the damage so far run between 500,000 websites to two-thirds of the Web but unless you are a bit of a technology junkie, the significance of Heartbleed will most likely have escaped you.

Technology still confounds many people. The speed at which it evolves and the exclusive code-speak that accompanies it ensures three consequences. First, that discussions of security in cyberspace are largely confined to the technical level. Second, that consideration of the strategic dimension of cyber security is lagging. And third, that a comprehensive approach to cyber security bridging the public/private and civilian/military divides that technology itself increasingly cuts across, remains wanting.

Nowhere in this region is this probably more apparent than in Southeast Asia. As Asean begins to coalesce into a community by 2015, the concept of physical, institutional, and people-to-people connectivity has taken on a greater urgency. Southeast Asia fares exceptionally well in the implementation of harmonised e-commerce laws with nine of the 10 Asean countries having laws related to electronic transactions and eight, to cyber crime. This is expected of a region that prioritises economic progress as the basis for political stability. However, as Asean looks to the future beyond 2015, it must begin to cast its eye -- however uncomfortably -- to the strategic dimensions of cyber security.

To be sure, Asean member states remain hampered by the digital divide, and limited human and financial capacity. But the lack of physical infrastructure now should not constitute an inherent restriction or excuse to lay an intellectual foundation and framework for the future, especially concerning strategic issues of cyber security. With commercial and military operations increasingly converging through shared skills and software in cyber space, there are critical questions that should be but have not yet been explored in depth in this region.

What happens in the event of a cyber attack against a nuclear power plant in, say, 2030 when Vietnam's generators are supposed to be operational? Or, if Malaysia's emergency services are disabled by malicious code simultaneously as a kinetic attack on a military installation? What recourse to action would be available? What level of attack would qualify as a use of force under international law? How would attribution be decided?

These questions sit uneasily with non-confrontational Asean member states not only because we eschew the slightest connotation of conflict but also simply because we do not consider these priority. However, if connectivity holds the key to Asean integration and community-building then the physical infrastructure that binds must be underpinned by the security of a governing framework which will lead to clarity of action in crises.

Moreover, if Asean is to be a credible convenor of discourse among our dialogue partners, many of which are major power players, then we will need to step up our intellectual game. It will no longer do for Asean to continue sitting back as neighbours in the Asia-Pacific proactively craft policies and approaches that will determine how the precepts, doctrines, and rules of strategic cyber security apply. Instead, Asean -- whether through the Asean Regional Forum or the Asean Defence Ministers

Meeting Plus -- will need to start grappling with evolving challenges in cyber space that impact upon fundamental precepts like state sovereignty and international law.

Cyber security is not simply about software bugs or code. Nor it is about monitoring or censoring Internet content. At the strategic level, it is about preserving security in a borderless domain where traditional divides between civilian and military, state and non-state, public and private, physical and virtual, and national and regional/international are increasingly being blurred.

This week, one of the top defence and security shows in the region -- Defence Services Asia 2014 -- opens in Kuala Lumpur. Its official programme of events includes a full-day conference on comprehensive cyber security, bringing together industry, policy, and the defence sector. Hopefully, this will be the conversation starter this region needs.

Elina Noor is ISIS Malaysia Assistant Director, Foreign Policy and Security Studies