NEW STRAITS TIMES ESTABLISHED 1845

June 2, 2017

# The fuzzy logic of cyberspace

By Elina Noor

LAST week, the Institute of Strategic and International Studies Malaysia convened the 31st Asia-Pacific Roundtable (APR), which was attended by approximately 260 local and international policy-watchers of the region.

As it has for decades, the APR deliberated in comprehensive fashion a number of strategic issues confronting the security of the region.

One of those discussions centred around emerging tensions in cyberspace between the private sector, on the one hand, and governments, on the other; the former, with its prioritisation of privacy and trust to catalyse technological innovation in order to capture an ever-growing market share, and the latter, focused on preempting, preventing, and defending against threats to national security.

Anchored by a majority panel of private sector players, it was an unconventional session that captured participants' attention (at least that of those who remained) for its currency and complexity. Participants stayed either because they actually understood the issues being discussed, or out of a desire to understand the fuzzy logic of cyberspace.

"Cyber" has become one of those buzzwords that people "get", yet don't really get. We understand how pervasive the cyber domain has become, given how much of our lives is spent on it, yet we do not fully comprehend the networks, systems, infrastructure, and above all, trust that underpin it.

We transact in cyberspace, yet we do not always grasp how the security of our data lies first and foremost with us. We realise how vulnerable we are in cyberspace, given how much of ourselves we divulge in it, yet we overlook just how much of our identity can be pieced together with enough motivation.

We entrust our data to the companies that store and transfer them, yet we are caught unawares when governments exploit vulnerabilities to mine that data for national security purposes.

Cyberspace and cyber security, therefore, are ethereal notions that we have come to accept in our lexicon, but have not yet begun to assume responsibility for or assign accountability to.

In large part, this is because unlike the natural domains of air, land, sea and space, the infrastructure of cyberspace — from fibre-optic cables to servers that maintain "clouds" — is man-made and, therefore, shared and governed by multiple stakeholders.

The private sector builds, owns, and maintains much of the physical infrastructure, or hardware, of cyberspace. Large technological multinational companies (MNCs) also provide the software that make up the soft underbelly of this super structure — from desktop programmes to mobile applications.

The size, revenue and influence of some of these giant MNCs dwarf smaller nation-states and economies. They operate across jurisdictions but have to comply with local regulations.

This means that they serve not only individual clients, but also governments that may have very different — and occasionally, conflicting — interests in using or leveraging the same products and services offered.

Companies that profit off cyberspace understand that trust in open, distributed programmes, networks and systems is key to making it all work.

Individual end-users expect that the information they send on invisible networks will be routed to and received by intended recipients in whole, rather than in part.

Until recently, as exposed by the Snowden leaks, there was also a certain naiveté that the privacy of this information would not be deliberately or accidentally compromised by the technology companies transmitting this information through the different states they operate in.

To say that borders do not exist in cyberspace is misleading. Data servers, for one, are physically located within a country's borders and protection of that data is subjected to laws governing that state.

Additionally, as with the Apple vs Federal Bureau of Investigation case last year, a nation's laws on free speech and privacy may determine the extent to which technology companies can guarantee data encryption.

They may also inadvertently afford mass murderers, terrorists, gang-bangers, and paedophiles, to paraphrase former FBI director James Comey, the opportunity to exploit encryption in the name of free speech.

What can be hard-hittingly borderless, however, is the impact of a government's interface with technological companies.

This was most recently demonstrated by the scale and spread of the ransomware WannaCry, which affected more than 10 nations as well as their critical national infrastructure, like the United Kingdom's National Health Service.

Although chiefly a criminal campaign despite rumoured links to a nation-state, WannaCry was drawn from — and its effects exacerbated by — a Microsoft vulnerability that had initially and allegedly been part of the United States' National Security Agency's offensive cyber arsenal.

This stockpiling by governments of what are called zero-day vulnerabilities, or programmatic flaws that are left undisclosed to be exploited to attack users, infrastructure, even countries, is shining new light on old frictions between technology companies and nation-states.

WannaCry showed that when giants collide in cyberspace, individuals end up paying in real life.

There are other important, strategic implications to be drawn from these unfolding developments, including how nation-states should behave with each other in cyberspace, what role the private sector should have in that debate, and whether a nuclear deterrence-like concept could work in cyberspace.

As technologically-advanced countries build up and boldly declare their offensive cyber capabilities, there are suggestions that the threat of mutually assured disruption will preserve stability in both the virtual and physical realms.

It is, therefore, critical that we begin to understand the multi-layered, overlapping nature of cyberspace, as well as the opportunities and inherent tensions that inextricably, yet, awkwardly connect its private, public and individual stakeholders.

*The writer is Director, Foreign Policy and Security Studies, Institute of Strategic and International Studies (ISIS) Malaysia*