malaymail online

November 28, 2017

Resilience and innovations for a diverse Asean

By Elina Noor

As the new chair of Asean, Singapore has announced that its thematic priorities for the region in the coming year will be resilience and innovation. This comes as little surprise given the island-nation's global trading status, technological advancements, as well as leading digital competitiveness and preparedness rankings.

Resilience and innovation in the region will be, to paraphrase Prime Minister Lee Hsien Loong at the closing ceremony of the 31st Asean Summit two weeks ago, premised upon a rules-based order. They will also be key to better dealing with emerging security challenges across the land, sea, air, and cyber domains.

The notion of resilience in the face of security challenges in cyber space has taken on particular importance in the West recently because of alleged interference in elections in the United States and Europe.

Amid histrionic accusations of nation-state manipulation of democratic processes and freedoms, there is the sobering reality of how states are to respond to information that may or may not be true but that nonetheless manipulates the latent cleavages of society.

For the multi-cultural nations of South-east Asia — not all of which are democracies — at least three cautionary observations stand out.

First, in case there was ever any doubt, information is power. That adage still stands. It takes on greater consequence in the information age where post-truth appears to be the new normal and mistruth speaks to power.

In South-east Asia, where the nation-building process is still unfolding, the challenges of online narratives among multi-ethnic and multi-faith societies are often under-appreciated.

Consider, for example, that Indonesia has about 14,000 islands with roughly 360 ethnic groups speaking over 700 languages and dialects. The Philippines has approximately 7,000 islands and around 70 ethnic groups speaking over 170 languages.

Myanmar has at least 135 ethnic groups. Laos, with a population of under 10 million, has 49 distinct ethnic groups, probably making it the most diverse country in South-east Asia on a per capita basis. In Malaysia, Sabah alone has 30 to 40 ethnic groups.

Building a shared national identity in each of these diverse South-east Asian states is complex enough on its own but is even more daunting in the digital age, where the amplification of rhetoric is tethered to the speed of connection.

Information that manipulates the core markers of social identity such as ethnicity and religion can fray the national fabric or rip it to pieces, regardless of its veracity. Remember that if radio was a major inciting vector of the Rwandan genocide, the instantaneity of the internet makes cyber space a more potent conduit of communalism.

Second, and this is important in light of the first point above, cyber space is just a vector. It is no doubt a uniquely potent medium because of the speed it offers for communication but misinformation and disinformation can only effectively exacerbate divisions that already exist in society.

Communal tensions exist in multi-cultural societies because of structural issues that have been allowed to fester. They are not suddenly manufactured simply because online users are liking, sharing, or retweeting bigoted assertions.

Fabricated information on social media inciting violence against Rohingya Muslims in the Rakhine state of Myanmar, for example, is a symptom and consequence of long-standing rancour left to fester.

Blaming social media is not a strategy and shutting it down would be pointless because there are countless ways to get around censorship.

Third, resilience is a whole-of-society effort. As the ultimate arbiter of national security, governments have a role in monitoring cyber space for threats. Less certain is how and to what extent governments alone should be exercising this role, especially since the state comprises more than just the government and it is the private sector that underpins most of the hardware and software of cyber space.

The US Congressional grilling of Facebook, Twitter, and Google at the end of October 2017 on the issue of election meddling showed just how important industry and technological players are when national and international security issues intersect in cyber space.

Placing the onus of responsibility wholly on corporate entities, however, is unrealistic given differing and sometimes, competing interests between public and private sector stakeholders.

The challenge for states is how to balance preserving the Internet's marketplace of ideas that allows innovation to flourish yet at the same time, ensure the resilience of society when confronted by attempts to pull it apart.

Part of the short-term solution lies in empowering Netizens with digital literacy skills so users evaluate the veracity of what appears on their news feed rather than unquestioningly absorbing what is presented. This is an area where the private sector can lead and contribute substantively, as Microsoft and others have already begun showing.

However, just as online problems are merely a reflection of deeper troubles offline, the bulk of rupture-proofing society in the long-term lies in addressing the structural causes of divisions. Many of these are rooted in parochial politics, inequitable economics, or educational flaws that fail to equip students with critical thinking and a wonderment about the world.

It will be up to the political leadership of each of the diverse nations of South-east Asia to bolster these aspects of resilience within the context of their own respective societies.

Singaporean academics who study crisis resilience short-handedly refer to society's ability to respond, adjust, and adapt to security challenges as its "bounce-back ability." In more ways than one, the Asean region will look to Singapore for leadership and support it in this term of art in 2018.

Elina Noor is director of foreign policy and security studies at the Institute of Strategic and International Studies (ISIS) Malaysia