NEW STRAITS TIMES

Tuesday, September 1, 2015

Be wary of what you say, the Internet can hear you

The control of radical thoughts in cyberspace comes from social engineering and is anchored in the real world, not in severing ties to information altogether

FARLINA SAID

IDEAS: *Cyberspace can amplify a message good or bad and propel it to influence many*

THE mediated environment is often regarded as innocent in its exchanges. Ideas are not dangerous, most would say. It is a great distance from playing violent games to committing acts of violence, studies have shown. However, violent extremism proves the distance is a lot shorter than one thinks. There are shortcuts in the human mind that ease the path for violent reactions. Ideologies persist even after headlines disappear.

If persistent messages are able to determine norms in the present community, then a message propagating and supporting violence or division in society encourages its practice in the everyday. In today's porous cyberspace, the control of such ideas is a question grappled by policymakers.

Yesterday, Peninsular Malaysia celebrated her 58th year of independence' with the 52nd anniversary for the formation of Malaysia coming this month.

The information environment of Malaya prior to independence had fewer actors. English newspapers catered mostly to the British colonisers with information for the business community and focused on European events.

Also present were press produced along ethnocentric lines, with the interests of each community at heart. The press can be beacons for ideologies that transformed the mind sets of Malaya. The public sphere that existed was, however, limited by the control of the British colonisers who did not wish to have their powers undermined.

Independent Malaya was little different. Born in a state of emergency, Malaya achieved freedom whilst fighting a violent insurgency. The public sphere then was contracted in comparison with the levels expected today. Cyberspace is perhaps the widest the public sphere has reached for Malaysia.

Theorists have likened cyberspace to a dimension much similar to that of air, land and sea. For security actors, cyberspace can expose vulnerabilities in computer networks and critical infrastructure. The transmission of information also shows the multitude of options for information

management; whether it be to keep it, steal it, to misinform or to propagate positive or negative convictions that divide an adversary's camp. Messages are subject to interpretation and that is dependent on the individual who consumes them. Ideological views exist offline and users bring these thoughts to the, Net.

The ability of the virtual realm to amplify a message can propel a single thought entrepreneur to influence many: Daniel Ventre, speaking of a State versus State model; imagines escalation that can occur in cyberspace until the core problem is resolved. The model begins with context as a starting point. The context can be long-standing systemic problems such as ethnic tensions. An event occurs in the real world, to which reactions manifest in cyberspace. Here, one will imagine an act of violence, a speech of racial hatred or the provocation of fear that polarises society. The live events are reinterpreted and discussed in cyberspace where decisions are reached and fed back into the conflict in the real world.

Should conflict continue in the real world, where the context has not been resolved, confrontations in cyberspace can multiply. The cycle of escalation occurs until the context is solved or the limits of the cyber conflict or the limits of the real world conflict are reached.

The finished process might leave behind traces of history, changed power relations or even a change in allegiance.

In order to seize control of the process either at the context level or in cyberspace, one's first thought might be to deny access or to stop the evolution of information. The antithesis of information disruption is usually by access limitation, either by using technology or through language. In China, for instance, content regulation is assisted by denial of service to sites, such as Reuters, Bloomberg, *The New York Times* and *The Wall Street Journal.* The vast majority of Chinese users also utilise local languages to communicate, which controls the dissemination of ideas. The language divide shapes an individual's experience of the Internet.

However, one needs to bear in mind that over-regulation does not solve core equations of context. Cyberspace, as the Internet has become tied to existing phone, fibre-optic and satellite systems, is not easily broken from its connection to people.

If there are three policy recommendations that can be made, it is to firstly identify the factors in the context. Without it, mediums such as cyberspace will only exacerbate real life events.

Secondly, is to dialogue with polarised mediums to develop a common understanding of national interest. To supplement the second step must be the creation of a united vision that draws on common values. Lastly is to encourage counter narratives that denounce violence. Not people dancing with parang, or waving a pretend-bloody keris or the encouragement to seek statements from those wishing to isolate others in the fabric of society .

Malaysia's independence was fought without bloodshed, and this message should reverberate in cyberspace and in reality. The control of radical thoughts in cyberspace comes from social engineering and is anchored in the real world, not in severing ties to information altogether.

The writer is an analyst in Foreign Policy and Security Studies at the Institute of Strategic and International Studies {ISIS) Malaysia