RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University

RSIS COMMENTARY

www.rsis.edu.sg No. 151 – 14 August 2017

Disinformation: Slow Burn Menace

By Shashi Jayakumar

Synopsis

Should state-sponsored disinformation campaigns be ranked as a national security threat on par with terror or cyber threats? How can the Singapore polity secure itself against such threats, and who should do what in the effort to shore up national resilience against this threat?

Commentary

RECENT DEVELOPMENTS should cause us to rethink what should lie within the scope of core national security issues. While terror and cyber threats are capable of causing great damage, it is increasingly evident that we should not neglect slow-burn issues that can be equally, if not more pernicious. A case in point is sophisticated disinformation campaigns and influence operations aimed at subverting the resilience of societies.

Some researchers think they have found fake Facebook groups almost entirely populated by bots. These fake groups, convincingly operated and orchestrated, leverage on existing filter bubbles and echo chambers, eventually attracting real fans. It is possible, as some researchers have posited, that many supporters of Donald Trump in 2016 on the presidential campaign trail were emboldened to declare their support for the candidate by the artificially-created perception of a swell in support for him. In this way, some of these originally-fake pages or groups swelled with real people, with the “fake” aspects of these groups withering away.

State Actors

The actual extent of Russian involvement in social media manipulation described above, or in influence operations aimed at affecting the outcome of the 2016 US

presidential election will be debated for years to come. What needs to be understood, however, is that these operations are simply one component of a suite that state actors employ to influence domestic affairs in other countries.

RSIS' interactions with experts in this field suggest that these tools can work synergistically or independently. They include conventional intelligence operations, cyber attacks, disinformation operations, leveraging on political allies, agents of influence and NGOs in the targeted country, support for local extremists and fringe groups, disenfranchised ethnic minorities, and economic operations with political goals.

Whether or not an influence campaign is state-sponsored, the nature of the disinformation is not static. Consider Germany, which has faced a spate of fake news on a range of issues from asylum seekers to information in support of anti-Islamist agenda. Just as it has clamped down on fake news through legislation, fact-checking websites and NGOs that put out correctives, the actors behind fake news appear to have evolved their methods somewhat.

There are indications that those behind fake news are beginning to evolve their methods in ingenious ways - telling fewer lies and more truths, with the same objectives and possibly even more success, using slant, interpretation, or weasel words. This has implications for how we should think about legal regimes – any legislation introduced in Singapore would have to be future proofed.

Antidotes and Conversations?

The countering violent extremism (CVE) experience had also taught us that the source of the countermessaging matters. Sometimes official sources are needed – trusted facts. But equally, this sometimes leads to the "backfire" effect – where one, confronted by a rational and fact-based rebuttal, is reinforced even further in his or her original beliefs. So too more generally with the whole fake news phenomenon.

What might work better in some cases – both with CVE and with fake news - is not official messaging. In both cases, the extremist or subversive messaging can out-evolve official counternarrative. What is needed just as much, if not more, are credible voices. Face-to-face contact also matters.

Extrapolating from this, it would be useful to consider the extent to which any initiative to combat fake news or disinformation can be successful if only the media and online platforms are used in the rebuttal. It could instead be argued that critical discourse in the real-world will be required in order to extract individuals from cognitive bubbles.

RSIS' contacts - particularly those who face the subversion threat with larger powers at their doorstep - have pointed out the importance of the need for governments to have open, frank discussions with the people about subversion. People thereby become attuned, but not paranoid.

Singapore saw the Our Singapore Conversation (OSC) initiative (2012-2013). Individuals involved in OSC dialogue sessions found it a useful thought exercise to come up against the sometimes very different views of their fellow citizens, helping all

concerned realise that their own worldview, however rational it seemed to them, was not the only one.

A Singapore Security Conversation?

Two suggestions come to mind. One would be using SgSecure, which has at its core national resilience, to talk openly about disinformation and subversion, and not simply terrorism. The second would be identifying grassroots actors and trusted authorities, and involving them heavily in the process.

Government need not and should not completely evacuate this space, but one wonders if taking some of the agency and putting it in the hands of people seen to be impartial arbiters (NGOs, could even be private sector – because they have to have a role) may have some additional inoculative effect.

Researchers from the Baltic states - which have become used to disinformation – point to the importance of investing behind the scenes in groups of people and to tackle disinformation within the community. In Europe, some of the key advocacy has been done by think-tanks. Some of their activities include publicly challenging supporters of Russian-sponsored disinformation, throwing light on the disinformation campaign vehicles, and systematically building social resilience.

In February this year, the Russian defence minister acknowledged the existence of a corps of Russian information troops, declaring at the same time that propaganda needs to be “clever, smart and efficient”. It can safely be assumed that many states are watching the Russian playbook with great interest.

SMART Nations as Tempting Targets

It is not just the big powers that have the means. Unlike traditional weapons, the technological and psychological tools to carry out these operations are available to nations of all sizes with the requisite technological capability and imagination.

More study is needed too on the particular effect that organised disinformation campaigns can have on states that are polyglot and multiracial, and which are also data rich – states that aim to be SMART Nations. These would be tempting targets.

Some of the best disinformation campaigns proceed long before they are noticed, and long before any kinetic action or visible damage occurs. Likewise the counteraction has to start in the same vein. We have to make a start.

Shashi Jayakumar is Head, Centre of Excellence for National Security (CENS), and Head of Future Issues and Technology (FIT) at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University, Singapore. A version of this appeared in The Straits Times.