RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University

RSIS COMMENTARY

www.rsis.edu.sg No. 312 – 23 December 2016

Society, Technology and National Security

By Norman Vasu and Benjamin Ang

Synopsis

As Singaporean society becomes increasingly and intimately interwoven with technology, a new national security challenge may emerge which Singapore will have to contend with.

Commentary

TECHNOLOGY BRINGS convenience even as it exposes societies to a wide array of risks. Many national security issues Singapore may face will emanate from the fact that our lives have fused with technology. Smart phones have become an extension of our brains, our devices watch our behavior as much as we watch them, and social media influences what we believe to be true.

This technological genie can neither be put back into the bottle nor should we attempt to be Luddites and avoid progress. As such, it behooves us to be aware of the possible dangers so that we can take steps to mitigate them.

Distortion of Perception

The viral spread of fake news and disinformation online gained international notoriety in this year's post-factual US Presidential Election campaign. A major state actor (Russia) has been accused of manipulating opinion and decision-making to create discord, uncertainty, and doubt, to achieve its political objectives – the same tactics it has been accused of employing against Estonia and Ukraine in the near past.

This is worrying because any other state, or terrorist group, can easily adopt these tactics anonymously in situations where they feel diplomacy would be ineffective and

all-out war would be too costly. Moreover, the tactics are also available to cybercriminals to exploit for profit.

While propaganda and psychological operations are old tactics of information warfare, social media groups have amplified their reach exponentially today, as each group self-selects and trusts its own messages, bypassing (and often rejecting) critical peer review, and supporting their own biases.

In these groups, teams of 'trolls' – malicious persons acting as group members – have completely bypassed mainstream media channels to create online persona, images, messages, videos, comments and campaigns that spread disinformation. These 'trolls' can be state-sponsored, or profit-driven (successful fake news websites earn substantial revenues from online advertisements), or even potentially artificially intelligent chatbots.

In addition, many social media platforms and search engines use computer programs and algorithms to filter what news posts or search results we see, generally to show us information which coheres with what we have liked before. This exacerbates the effect by creating filter bubbles or echo chambers where conspiracy theories thrive and facts can be dismissed. German Chancellor Angela Merkel called them out this year for this lack of transparency that "distorts perception".

Facebook is now trying to combat the fake news plague. But many, even in technology-savvy Singapore, still do not recognise that their Facebook news feeds and Google searches show them the most popular results, not necessarily the most truthful or accurate ones.

Beyond Disinformation

Disinformation tactics are sometimes accompanied by cyberattacks, like the breach of the Democratic National Convention email servers this year, or the persistent low-level attacks on Estonia's ministries, banks, and media in the past.

As the Internet connectivity and mass transport breakdowns this year reminded us how much Singaporeans rely on technology in daily life, we wonder if our highly-connected citizens, used to efficiency and stability, may be ill-equipped to deal with a slow drip degradation of services, especially if accompanied with fake news campaigns sowing discontent.

Even without cyberattacks, opportunistic adversaries can exploit societal changes with fake news. As the Fourth Industrial Revolution continues at pace in our technologically driven society, with artificial intelligence and automation replacing human work, many blue and white collar jobs may be eliminated forever. As a society, we need to ensure that economically displaced citizens are kept meaningfully engaged, lest they become vulnerable to misinformation campaigns promoting xenophobia, extremism and scapegoating.

Developing Resilience

Since attempts to spread fake news cannot be avoided, a great cyber wall cannot be

created to protect us from every cyberattack, and the changes to society brought about by fast-paced technological change cannot be stopped, the best solution is to develop resilience all through society to mitigate these challenges.

At the individual level, resilience can be found through the learning of new enhanced skills of media literacy and critical thinking to deal with the new deluge of information. These are skills enabling Singaporeans to both discern between truth and falsehood online and to avoid contributing to the spread of falsehood and distorted information.

At the community level, we can build our cyber resilience by training to respond to attacks, just as we have fire drills and emergency drills today. At the industry level, beyond maintaining robust cybersecurity measures, businesses can build resilience by training to respond to breaches, and by maintaining backup systems that can be called upon in times of emergency.

Finally, at the state level, the government plays the key role of chief coordinator to encourage the development of resilience within society towards these new national security challenges. Overall, the social and technological challenges of the future cannot be avoided, and should certainly not be feared, but should be prepared for.

Norman Vasu PhD is Deputy Head of the Centre of Excellence for National Security at the S. Rajaratnam School of International Studies, Nanyang Technological University, Singapore. Benjamin Ang is Coordinator of the Cybersecurity Programme in the same Centre. This appeared earlier in TODAY.
