Written Representation 46

Name: Dr Liew Kai Khiun
        Assistant Professor
        Wee Kim Wee School of Communication and Information
        Nanyang Technological University

Parliamentary Submission to Green Paper on "Deliberate Online Falsehoods: Challenges and Implications" Mis 10 of 2018, Order of Parliament to lie upon the Table 5 January 2018 by Dr Liew Kai Khiun

Dr Liew Kai Khiun, 26 January 2018

1. This parliamentary submission is a response to paras. 84 and 85 abovementioned Green Paper that is listed as the following:

   84. The Government therefore intends to ask Parliament to appoint a Select Committee to examine and report on:
   (a) The phenomenon of using digital technology to deliberately spread falsehoods online;
   (b) The motivations and reasons for the spreading of such falsehoods, and the types of individuals and entities, both local and foreign, which engage in such activity;
   (c) The consequences that the spread of online falsehoods can have on Singapore society, including to our institutions and democratic processes; and
   (d) How Singapore can prevent and combat online falsehoods, including:
   i. The principles that should guide Singapore's response; and
   ii. Any specific measures, including legislation, that should be taken.

   85. The public will be invited to make submissions to the Select Committee on these issues, once Parliament approves the formation of the Select Committee. The Select Committee can also hold public hearings, to engage in-depth with witnesses on key issues.

2. The purpose of this submission is to propose a **calibrated** approach towards the **context and extent** in which Singapore should respond to the threat of the systematic campaigns of disinformation particularly through the cyberspace. Within the rapidly evolving geopolitical and technological landscapes, it seeks in finding a careful balance between freedom of information and speech, critical to a functioning economy and progressive society and the public security and social cohesion that concerns the survival of the city-state.

3. The author appreciates the perspectives of different parties pushing for more stringent measures against those who purport "fake news" against those with reservations on the arbitrary potentials that may open the system to political abuse. The latter argues that the best solution to combating fake news is not repressive measures, but more free speech to expose and counteract them. In his scholarly commentary on libel action against anonymous internet trolls, the communications lawyer Charles Insler (2016) opines:

   "More speech also promotes the general rule that "the best test of truth is the power of the thought to get itself accepted in the competition of the market." The best response to a troll's comments is not to reinforce them through litigation, but to weaken them through additional discourse or no discourse at all. We should remain faithful that ideas of merit will eventually take root and that falsehoods will meet their winter and wither on the vine" (5).

   While agreeing with this principle broadly, the author feels a more contextual approach is needed instead of leaving information to correct itself in the marketplace of ideas. The visible hand of particularly the state is needed here in a time when information flows are being systematically manipulated by external parties with intentions misinform rather than inform.

4. The 2016 American Presidential Elections have highlighted the significance of the vulnerabilities of even a superpower in systematic cyber-subversion by suspected foreign influences seeking to exploit and magnify existing social divisions actively. Known as internet trolling, such has entailed the institutionally supported acts of using both human agents (usually operating under multiple online fake accounts) as internet trolls and internet bots (software applications that runs automated tasks) in infiltrating, inflaming, and overwhelming existing national discussions in social media platforms with intends to sow social discords and sway public agendas (Leo, Arif and Starbird 2018). So far, Singapore has yet to be affected adversely by such tactics. In framing such methods along military lines, Stephen Hart and Mark Klink (2017) have coined the term of "Offensive Troll Operation", one that:

"...identifies weaknesses in the adversary's cyber-persona's narrative, information mediums, or access to information to deny, degrade, or disrupt their adversary's ability to conduct combat operations and to shape the adversary's social and political environment... Foreign governments using a combination of state sponsored media and influencers who support their positions on social media disrupt the free discourse of ideas in American media and life. The influencers who aggressively weaponize information on social media are known as trolls. The language reuses a term formerly meant to denote a person who disrupted UseNet online discussion lists via derogatory and off-topic remarks (97)."

Guarding against such operations entails what Hart and Klink (2017) term as the "Defensive Troll Operations-Identifies, destroys and neutralizes foreign trolls operating on the cyber-personas of American leaders, institutions, and persons." For them, this covers not just the online identification, exposure and deletion through the same human and computer generated systems, but also the boosting of support for groups opposing such offensive operations (101-102). Singapore has yet to fall victim to such extensive troll operations. Aside from the fact of being a small country with little significant limelight in geo-political stage, this author considers a mixture of an active government coupled with a highly savvy netizenry that have protected politics and political discourses from external manipulation.

5. However, vigilance is still needed as such activities, however undercurrent, can pose potential dangers to the republic. For example, one witnesses the constant barrages of comments by seemingly Myanmar based user-accounts on the social media news portals related to the Rohingya issue. This includes that of Singapore's mainstream news networks like Channelnewsasia and the Straits Times. Although some can be independent individual postings, the volume of the posts from the "denialists" aiming to discredit Singapore's newsnetworks, suggest a more systematic effort from an organised external source. These inflammatory contents with even Islamophobic tones, have occasionally created online backlash from Singaporean Muslim accounts resulting in heightening tensions along religious and ethnic lines. Left unmonitored, such undercurrent tensions may increase Singapore's vulnerability to social discord that can be easily exploited by external bodies. Figures 1 and 2 from the screenshots from a Channelnewsasia (2017) report on the Rohingya issue by Afifah Ariffin on 15 September 2017 has generated heated barrage of responses from seemingly Burmese user accounts that collectively degraded the quality of the discussions and overwhelmed the particular site with more socially toxic tones with exchanges with users that are seemingly from Singapore.
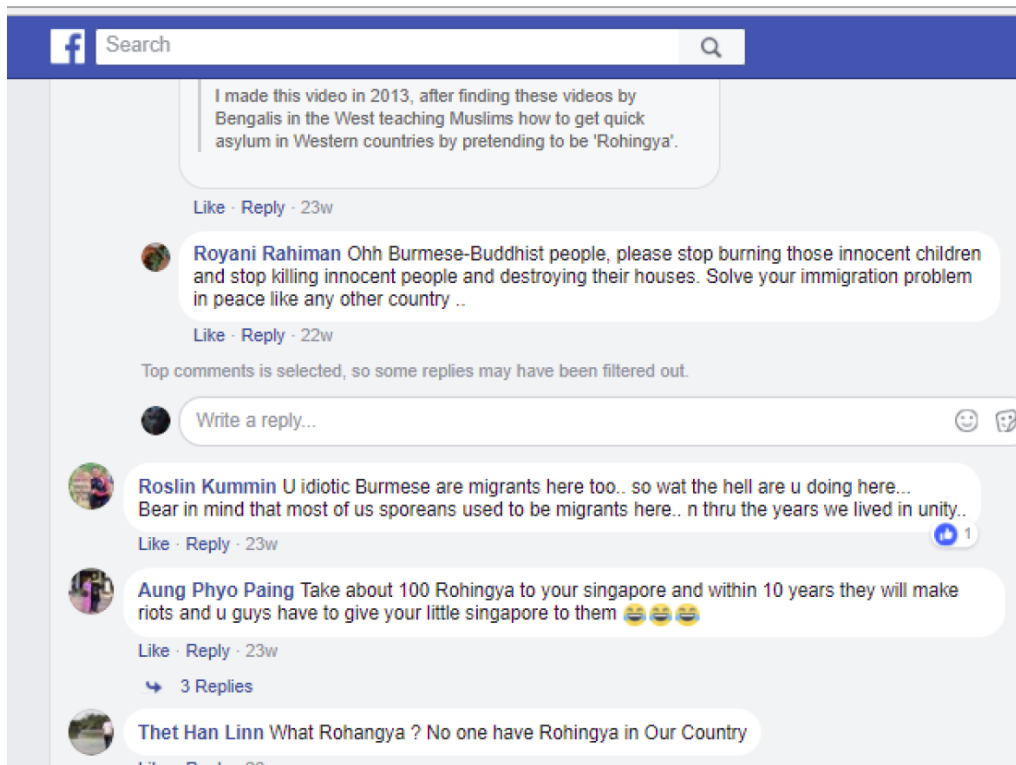
Figure 1: Screenshot 1 of comments from Channelnewsasia report 15 Sep 2017
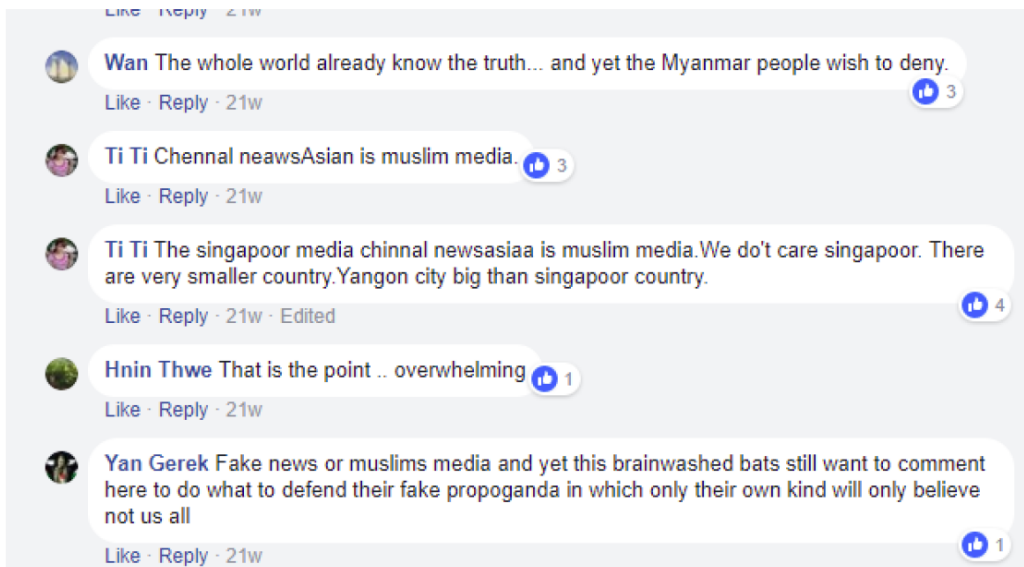

Figure 2: Screenshot 2 of comments from Channelnewsasia report 15 Sep 2017

6.   Table 1 is a proposed template for the deployment of a more calibrated approach towards handling systematic disinformation tailored broadly along differing contextual scenarios. Analogous to a traffic light, the three levels, "Green", "Yellow" and "Red" suggest a graduated response mechanism that the authorities should undertake along the severity of the situation. Rather than a "one size fit all" approach that is both administratively and politically disproportionate, a more nuance perspective is needed.

Table 1: The Traffic Light Approach to countering Disinformation.

Code	Scenarios	Examples	Suggested actions
Green	Normal	The case of the trolling activities by The Real Singapore in the "Thaipusam incident" in 2015. Burmese "Defensive Troll Operations" seeking to systematically dominate and mis-represent the Rohingya issues in international news sites, including that of the Straits Times and Channelnewsasia.	a. Targeted use of existing media and other civil regulations like Sedition Act as well as the discretionary application on political pressure (persuasion and dissuasion on concerned individuals). b. Requirement for media and social media networks to flag and weed out incidences of Offensive Troll Operations on their sites.
Yellow	**Incidences & Events**	**General/Presidential Elections, episodic occurrences (i.e. SARS in 2003; Little India Riots in 2013)**	a. **Banning all political parties and candidates on the use of Offensive Troll Operations particularly the engagement of foreign agencies, commercial or otherwise.** b. **Reporting, eradicating and even closing down of networks and platforms suspected of being infiltrated by foreign Offensive Troll Operations.** c. **Outlawing Singapore citizens and foreign nationals in Singapore from supporting and engaging foreign Offensive Troll Operations targeting the republic during such incidences.**
Red	**State of Emergency**	**Nation under direct external threats and internal strife, i.e. case of gulf states against Qatar in 2017 and food shortages in Venezuela .**	a. **Extension of prevention detention ordinances under the Internal Security Act (ISA) to actual persons involved in systematic Offensive Troll Operations.** b. **Restriction of information flows**

7. As reflected in Table 1, "Code Green" operates under a situation of normality characterized by both sporadic acts of disinformation and mild Offensive Troll Operations. The absence of any significant incidents reduces that of the vulnerability of Singapore to such exploitation, and while individual culprits should be held criminally accountable under existing regulations, the freedom of information and discussion should not be hindered. "Code Yellow" should apply to more heightened incidents, either planned like national elections, or incidences like the "Little India Riot" that requires a more conscious approach in strengthening the mechanisms of Defensive Troll Operations.

8. Here, what is of most concern to the author is the potential engagement by political parties during national elections of especially foreign agencies and contractors to serve their political campaigns. While such practices may gain short term political mileages, the long term effects from internally commissioned external cyber-disinformation efforts can have damaging long term implications as some research has demonstrated (Cabañes & Ong 2018). Hence, **one proposal in this submission calls for the prohibition of the use of Offensive Troll Operations tactics and services by political parties and politicians and social influencers during the times of national elections perhaps under the Elections Act.** Lastly "Code Red" denotes the context of a situation of a "state of emergency" whereby the cyberspace, like the physical space and, netizens, like citizens should be expected to comply with restrictions arising from any national crisis. In this respect, any preventive detentions under the Internal Security Act should be universally applied to subversive elements in both the real and virtual worlds. In both the situations of Codes "Yellow" and "Red", the author would also suggest extensions of laws against Singapore citizens and foreign nationals contracted by foreign agencies in Offensive Troll Operations against Singapore.

9. In conclusion, in striking a balance between ring-fencing Singapore against real foreign threats of Offensive Troll Operations and protecting the freedom of information and discussion vital to the republic's progress, this submission argues for a more calibrated approach towards combating misinformation and fake news. Depending on the prevailing contexts, the various proposals raised in this submission call for greater awareness in such Offensive Troll Operations as well as a range of preventive legal and administrative measures to prevent them from taking root in Singapore.

References

Cabañes, Jason and Jonathan Corpus Ong (2018). *Architects of Networked Disinformation: Behind the Scenes of Troll Accounts and Fake News Production in the Philippines*, The Newton Tech4Dev Network and University of Leeds. http://newtontechfordev.com/wp-content/uploads/2018/02/Architects-of-Networked-Disinformation-Full-Report.pdf

Channelnewsasia (2017). "Many of the #Rohingya refugees fleeing the crisis in Rakhine are living in makeshift camps in Bangladesh. Channel NewsAsia's Afifah Ariffin reports from one about 3km from the Myanmar-Bangladesh border." 15 September 2017. https://www.facebook.com/ChannelNewsAsia/videos/10154974493317934/?hc_ref=ARSBm7TqdotiwICmSMxlccvHL2wzm0mcsYSopAZ2EPSYnnLeiX3dqypaZy6oRvJz2Wk

Hart, Stephen and Mark Klink (2017). "1st Troll Battalion: Influencing military and strategic operations through cyber-personas". *International Conference on Cyberconflicts, 2017.* 97-104. DOI: 10.1109/CYCONUS.2017.8167503

Insler, Charles (2016). In (Partial) Defense of Internet Trolls: Advocating a Flexible Summary Judgement Standard before Unmasking Anonymous Commentators Accused of Defamation*", Publication of the Forum Committee on Communications Law, American Bar Association*   ;   32(1):   9-14. https://search.proquest.com/docview/1792391209?accountid=12665

Ministry of Law (2018). Deliberate Online Falsehoods. Challenges and Implications. A Green Paper by the Ministry of Information and Communication and the Ministry of Law. https://www.mlaw.gov.sg/content/dam/minlaw/corp/News/Annexe%20A%20-%20Green%20Paper%20on%20Deliberate%20Online%20Falsehoods.pdf

Steward, Leo, Ahmad Arif and Kate Starbird (2018). "Examining Trolls and Polarization with a Retweet Network", *MIS2: Misinformation and Misbehavior Mining on the Web.* https://faculty.washington.edu/kstarbi/examining-trolls-polarization.pdf