Select Committee on Deliberate Online Falsehoods
Summary of Evidence - 16 March 2018 (Day 3)

1. The Select Committee on Deliberate Online Falsehoods held two private sessions today to hear oral evidence. These sessions were held in private because they concerned matters of national security and international relations. The other sessions were in public.

2. This summary also contains the summary of the evidence from Mr Septiaji Eko Nugroho (Mafindo), Dr Elmie Nekmat, Ms Myla Pilao (TrendMicro) and Mr Morteza Shahrezaye.

Private sessions

3. Dr Gulizar Haciyakupoglu and Dr Damien Cheong shared their views on how information warfare can and has been used against Singapore.

Dr Gulizar Haciyakupoglu

4. Dr Haciyakupoglu's evidence was as follows:

   i. Disinformation campaigns have become more sophisticated with disruptions in technology and media ecology and changes in news consumption habits.

   ii. States who mount these campaigns have an unrestricted approach to warfare. They do not separate between wartime and peacetime. They do not distinguish between what is military and what is not. Nothing is off the table.

      (a) The types of warfare used include psychological warfare, where efforts are made to shape public opinion. The aims are to paralyse public policy decision making and undermine a society's confidence in itself.
      (b) Civilians are not just victims in disinformation campaigns which are a part of psychological warfare. They participate as circulators of disinformation and misleading content creators.
      (c) Civilians can even be part of a militia that acts in support of a state sponsored disinformation campaign.
      (d) States use civilians to achieve these outcomes as this allows them to avoid any blame in the domestic or international arena.

iii. Such disinformation campaigns are complemented by cyber-attacks which include malware attacks, Distributed Denial of Service attacks and integration of "backdoors programmes". These cyber-attacks allow the aggressor states to collect information on the target country's citizens, to guide their online actions and increase their impact. All these can be orchestrated remotely by employing civilians.

iv. Online efforts are also reinforced by offline efforts which spread influence.

5. Dr Haciyakupoglu gave the specific example of two countries, which for reasons of confidentially will be called X and Y. Country (X) which has taken efforts to infiltrate another society (Y) through several methods, including disinformation campaigns.

i. X embraces an unrestricted approach to warfare. This gives a continuous nature to information operations and blurs the boundary between information operations and information warfare (which is the subset of information operations waged in times of war or conflict).

ii. X's information operations are mainly waged in the information domain, and encapsulates "subdomains" such as "the computer network domain," "the electromagnetic domain," "the psychological domain," and "the intelligence domain." Within this framework, online and offline endeavours, and actions in the sub-fields of information domain complement one another.

iii. X has used various methods including disinformation campaigns, psychological weakening, manipulation of public opinion, and tactical campaigns.

iv. X has utilised civilians in Y in its disinformation efforts through three means. First, it has manipulated the media in Y, by using media professionals (on mainstream media) and content creators (on social media). Second, X has a state agency that spreads influence in Y with the help of businessmen, students, academics and other groups. Third, X carries out cyber-attacks with the help of civilians (so that there is no direct link back to X).

v. As a result, country Y has been thoroughly penetrated, even though Country Y has taken some countermeasures.

6. The threat is real for Singapore.

i. There have been a number of occasions when Singapore has been subjected to cyber-attacks in the recent past, including attacks on sensitive ministries.

ii. There are also some indicators of information warfare being practiced against Singapore in recent months. This involves a state putting its perspective on the table, through news articles and social media for instance, to try and influence the minds of specific segments of the affected society. This is to legitimise the state's actions on an international sphere.

7. Cyber-armies exist in Malaysia, Indonesia, Vietnam and other countries in the region.

Dr Damien Cheong

8. Dr Cheong's evidence was as follows:

i. Disinformation campaigns are a serious problem.

ii. The goal of a state-sponsored disinformation campaign is to destabilise the government and society of a target country. Such campaigns can take the form of a short or long game.

(a) A short game is where the misinformation creates crises for the target, and

(b) A long game is where the misinformation exacerbates existing crises, and creating more serious ones in the long run.

iii. There are four main challenges when dealing with such disinformation campaigns:

(a) The overload of information in today's world confuses individuals, who then resort to cognitive biases (like confirmation bias and popularity) to decide what information to believe.

(b) Disinformation campaigns will be carried out on the offline, as well as online world.

(c) Singaporeans could become involved in such disinformation campaigns in three ways. First, they may do so knowingly. Second, they may duped

or co-opted into unknowingly participating in such disinformation campaigns. Finally, they may simply share the misinformation without any malicious intent.

(d) The spread of misinformation via encrypted messaging apps like Whatsapp and Telegram is also of concern, as it increases the spread of the misinformation.

iv. Singapore is not yet prepared fully for the methods by which such attacks take place.

(a) There are cyber-armies in the region including Malaysia and Indonesia. These can be easily deployed against us directly or as proxies for another country.

(b) There will be instances when public institutions will be targeted. For instance, actors will target the police which is a highly trusted institution in Singapore. Incidents could be created to generate distrust against the police. Such incidents have been generated. Undermining trust in the police force will undermine trust in the state.

(c) Individuals need to be careful about the use of phones which have been manufactured by companies based in foreign states. Many are likely to have back end access to foreign intelligence agencies.

v. It is necessary to prepare our responses on two levels, public measures and private steps. Our system has to build both defensive and offensive measures. We also need substantial amendments to legislation, including security legislation. These are necessary to prepare for the threats. We need Total Defence.

Septiaji Eko Nugroho (Mafindo)

1. Mr Septiaji Eko Nugroho spoke on the Indonesian experience with Deliberate Online Falsehoods.

2. His evidence was as follows:

i. Falsehoods spread easily among Indonesians because of (a) low literacy, (b) polarisation between people of different ethnic, religion, political affiliations and economic status and (c) partisanship of mainstream media.

Disinformation can also be spread by or impact those with high education and a well-paying job.

ii. Indonesia is not spared from falsehoods:

(a) In 2016, false information that a Chinese woman was angry with the call for morning prayers was spread via chat apps in North Sumatra. This resulted in a mob destroying several temples and pagodas.

(b) In 2017, fear mongering rumours spread over social media and chat apps about a massive child kidnapping operation in Indonesia. This false information had the police logo on it, causing people to believe it. This led to a father being wrongly beaten to death by a vigilante mob in West Kalimantan.

iii. On motivations, he observed that Indonesians spread falsehoods for economical, political and/or ideological reasons.

(a) Sometimes financial gain can converge with political motivation in the creation and spread of falsehoods (e.g. Indonesian police had apprehended members of a group known as Saracen for being paid to spread political falsehoods).

(b) In Indonesia, disinformation spikes near major elections, and this started with the Jakarta governor election of 2012 and has continued since. Misinformation tends to be higher in in areas where there are racial, religious tensions.

iv. While Indonesia has not witnessed the spread of falsehoods by foreign actors, this may be because Indonesia uses Bahasa. However, this means that countries with a widely used language as the main language (like English or French), should be prepared.

v. Singapore is also at risk from falsehoods.

vi. In terms of efforts to engage technology companies, while there is some support from technology companies to flag false stories, nevertheless often it is difficult to get them to cooperate. Google, for example, has not agreed to take down any content, even if false, citing “net neutrality”. Government should be able to require technology companies to take down content that is incendiary in nature. Indonesia has legislation that gives it some powers

to deal with falsehoods and incendiary materials. Mafindo has recommended more legislation.

Dr Elmie Nekmat

9. Dr Elmie spoke about the necessity of both regulation and education-based efforts to combat deliberate online falsehoods.

10. His evidence was as follows:

i. Deliberate online falsehoods can be done over a period of time. But, the effects of deliberate falsehood and misinformation in social media can also occur rapidly, and impact broad segments of society within a short period of time.

(a) Such effects tend to be the outcomes of finely calibrated disinformation campaigns carried out on social media.

(b) They are aimed at influencing election outcomes, influencing public debates on domestic policies.

(c) The speed in which such disinformation spread reveals limitations of public education and media literacy efforts.

ii. It is necessary to consider relevant regulations which compel digital content distributors to prevent the flow of deliberate misinformation on their platforms.

(a) This would cover technology companies, which are major conduits to the development and spread of online falsehoods.

(b) Making such content distributors accountable sends a clear signal to them that stopping online falsehoods from reaching others is their responsibility.

iii. In Singapore's context :

(e) Deliberate online falsehoods can harm our multiracial society.

(f) We should not blind to the potential of falsehoods stoking ethnic and religious tensions amongst Singaporeans, just because no racial conflicts have occurred.

(g) There needs to be more relevant forms of regulations, educational initiatives as well as greater research and studies into the problem.

iv. The role of language is influential in the dissemination of falsehoods. Influence can come from neighbouring countries like Malaysia and Indonesia. This can also apply to selected Chinese dialects and other languages. For example, on closed platforms such as WhatsApp, messages that are more relatable to a particular group or a particular can be spread easily.

v. There are varying levels of awareness among the Malay community itself about falsehoods. The younger generation is more aware because of national debates such as this. They are more knowledgeable about how falsehoods are created and its negative impact. On the other hand, this is less so for the older generation. The debates and examples provided in relation to falsehoods are all in English. Therefore, it is hard for the older generation to understand them.

i. If the current laws are insufficient, they should be ramped up to deal with content producers who deliberately sow discord among society.

Ms Myla Pilao, Trend Micro

1. Ms Pilao spoke about the methods and ease in which fake news can be created and spread online today.

2. Her evidence was as follows:

i. It is difficult to distinguish real from fake news, as cyber-propagandists use proven and reliable techniques each time.

ii. Fake news can be used to attack businesses, and hoodwink consumers.

(a) Companies can post false, negative comments about competitors on review websites.

(b) An individual has also tricked people into believing his garden shed was a top-rated restaurant on TripAdvisor.

iii. It costs significantly less to spread fake news than to post legitimate advertisements or paid content. There are various tools and services

(legitimate and illegitimate) commonly found in underground or even gray markets, for people to spread fake news. For example:

(a) There are content market services which can be cheaply obtained. For just US$15-$30, fake news operators can obtain fake articles.

(b) Fake news operators can influence the outcome of polls or elections using "click farm services", for just a few thousand US dollars.

(c) One can buy 1 million Instagram likes for $18, and shape the way information is conveyed on that platform.

(d) A street protest can be instigated in the US for just US$200,000.

iv. Social networks are key to the spread of misinformation.

(a) Facebook, given its number of users, is the most likely platform of choice to launch fake news campaigns.

In Twitter, information is also spread through "gurus" or "sect followers", who have a large number of followers. They simply retweet content generated by others, and do not create new content.

(c) Many operators use humans now instead of bots to spread fake news, as bots are now easier to identify. It is difficult to distinguish bot-generated content from content generated by a genuine user.

v. Cyberpropagandists are likely to follow a public opinion cycle – an 8-step process to change public opinion and spread fake news:

(a) Reconnaissance – gather info and analyse target audience. A lot of research is done at this stage.

(b) Weaponization - prepare the key story of facts they wish to spread, and create background stories to support, and alternative versions to plant to trick informed readers.

(c) Delivery – use available tools and services to spread quickly across traditional and social media.

(d) Exploitation - controlled, targeted promotion done among small but active groups of supporters, such as on social media.

(e) Persistence - reach critical mass in terms of supporter volume. This can be done using legitimate (such as buying advertorials) and illegitimate tools.

(f) Sustainment - keep story going while anticipating and reacting to changes in sentiment;

(g) Taking Action - if public sentiment change, need to take necessary steps to get back on track;

(h) Trace Removal - once mission is accomplished, need to switch the public attention somewhere else, so they will not fall under public scrutiny. This can be as simple as removing items or keeping themselves low. Cyber criminals use multiple accounts and identities to make it difficult to trace them.

vi. Countermeasures should comprise a suite of measures, and legislation can be a good solution. Different types of responses should be used for different types of misinformation and threats.

Mr Morteza Shahrezaye

3. Mr Shahrezaye spoke on the increasing use of social media for political discourse.

4. His evidence was as follows:

i. Today, there is a strong trend towards bringing more political discourse onto the social media.

ii. However, social media platforms are not designed for political and democratic debate; they are better designed for private use. Social media is designed for communication guided by private affinity and emotions. Political debate on the other hand requires a certain structure for effective debate.

iii. Social media and technology have caused a blurring of the private and public sphere. And this can affect democracy quite seriously.

iv. Social media can be manipulated to create a false impression of the popularity of a specific opinion. This can cause people, including journalists and politicians, to fall for the wrong trends and make bad decision.

(a) It can change political agendas. If there is a person who is not yet decided on an issue, e.g., refugees, the user might be influenced by manipulation. Political debate in Germany on immigration has been negatively impacted by online falsehoods. Dr Shahrezaye also said that there is no conclusive evidence yet whether political opinions in Germany have been influenced by online falsehoods.

v. The algorithms on social media can take on the active social media debate on an issue, generated by bots, and spread it widely.

vi. In the long run, social media manipulation may amplify existing tensions and lead to polarisation. This can result in, among others, less social respect for each other and people having more extreme points of views.

vii. There has to be responsibility on those who bring the private field into the public. These would include the originator of the news, those who share and the technology companies which widely distribute the news. Governments can though regulations require technology companies to bear responsibility for the distribution of falsehoods. Fines can be imposed. Technology companies can also be required to be more transparent about how their algorithms work to show what would be the consequences in terms of consumption of news.