Written Representation 59

Name: Shashi Jayakumar
Head, Centre of Excellence for National Security & Executive Coordinator, Future Issues and Technology, S.Rajaratnam School of International Studies, Nanyang Technological University, Singapore

Received: 27 Feb 2018

Submission to Parliamentary Select Committee on Fake News

Shashi Jayakumar, Head, Centre of Excellence for National Security & Executive Coordinator, Future Issues and Technology, S.Rajaratnam School of International Studies, Nanyang Technological University, Singapore

Disinformation/Fake News Campaigns and Their Implications

We live today in a unique age. A technology tsunami has enabled algorithms with the ability to harvest on social media platforms an enormous amount of information about us. These can record, analyze and accordingly anticipate our preferences (and sometimes needs) even better than we do. With ten Facebook "likes" as inputs, an algorithm predicts a subject's other preferences better than the average work colleague, with 70 likes better than a friend, with a 150 likes better than a family member and with 300 likes better than a spouse. [1]

This means that for political actors – both state and non-state – seeking to influence opinion and subvert societies, myriad possibilities are now open. Instead of banal, generalized advertisements of the past, messaging can target individuals in persuasive, highly individualized forms. Since there was no need to appeal across the board, targeting at the individual level has corroded the democratic process.

Modern information technologies empower and incentivize subversion at scale. In cyberspace, there is no requirement of course for messages to have a direct connection to the truth, and, either way, the perpetrator of falsehoods can mask its tracks and have some degree of plausible deniability. Why not then employ these techniques to undermine resilience in targeted countries, when these methods can be far cheaper (and less bloody) than warfare, and which may be more precisely tailored to achieve state aims compared to diplomacy? It was after all Sun Tzu who observed that to subdue the enemy without fighting is the acme of skill.

---

[1] Wu Youyou, et.al., "Computer-based personality judgments are more accurate than those made by humans,", Proceedings of the National Academy of Sciences of the United States of America, January 2015, 112 (4), pp.1036-1040. http://www.pnas.org/content/112/4/1036.full

[2] Jakub Junda and Ondřej Kundra , 'Mechanisms of Influence of the Russian Federation into Internal

Techniques and Tactics

General Valery Gerasimov, Chief of General Staff of the Russian Armed Forces, has observed, "the information space opens wide asymmetrical possibilities for reducing the fighting potential of the enemy". A great deal of what Russia has tried in the European Union and its former satellites in Europe has disinformation at its heart. Spreading rumours to discredit politicians (and to play up certain themes – such as negative portrayals of immigration policy) have been aimed at undermining public trust towards democracy and systematically influence populations to become less trusting of mainstream, established news networks. Instead they would put more trust on fringe sources of news (often backed by Russia) and conspiracy narratives.[2]

This has also been on view in the United States. The full story of what exactly Russia attempted in terms of opinion manipulation in the 2016 US Presidential Election will probably not be apparent for some time to come. However, the scale and ingenuity were striking.[3] Some researchers think they have found fake Facebook groups almost entirely populated by bots. These fake groups, convincingly operated and orchestrated but operated by bots and AI, leveraged on existing ideological filter bubbles and echo chambers, eventually attracting real fans. It is possible, as some researchers have posited, that many Trump fans were emboldened to declare their support for the candidate by the artificially created perception of a swell in support for him. And in this way, some of these originally fake pages or groups swelled with real people, with the "fake" aspects of these groups withering away.

It would be a mistake to assume that Russian intervention in the US 2016 presidential election (and continued meddling since) has been solely to

[2] Jakub Junda and Ondřej Kundra , 'Mechanisms of Influence of the Russian Federation into Internal Affairs of the Czech Republic', European Values Think Tank Study. 4 Sep 16. http://www.europeanvalues.net/wp-content/uploads/2016/09/Mechanisms-Of-Influence-Of-The-Russian-Federation-Into-Internal-Affairs-Of-The-Czech-Republic.pdf

[3] On the issue of scale: Facebook has disclosed that pro-Russia ads reached out potentially to 126 million users, while Twitter has – belatedly – exposed over 2700 accounts that were tied to the Kremlin-linked organ, the Internet Research Agency. 'Lawmakers release trove of Russian-linked Facebook ads, Twitter handles', *CBS/AP*, 1 Nov 17. https://www.cbsnews.com/news/lawmakers-release-trove-of-russian-linked-facebook-ads-twitter-handles/

support the Trump camp and to shore up the "Alt-Right". Some of the rumours and untruths carried by bots and fake ads supported and inflamed all sides of the political spectrum, (Pro Trump and Clinton, the alt-right as well as the candidacy of Bernie Sanders, pro and anti LGBT). As one knowledgeable observer commented, "The Russian bots and trolls aren't just pro-Trump […as long as they're fomenting division and chaos] they don't really care."[4] It seems, as in Europe, that the methods were used not so much s to strengthen any one cause, *but to create dissension and undermine the resilience of the polity.*

There exist individual "consultants" and private sector entities specializing in hacking or interfering with elections with the aim of achieving the desired election result for the client. Their methods include smears, hacking, spoofing webpages, and sending mass emails to influence outcomes. [5] More broadly, there also appears to exist a growing shadow market for methods to influence target populations – and outcomes - in nations, using methods like those offered by Cambridge Analytica, the company said by some reports to have profiled, and micro targeted, the US electorate during the 2016 presidential election.[6]

"Information Troops"

Military doctrine of major powers evolved to encompass the notion that information and propaganda are just as important as "kinetic" modes of

[4] Denise Clifton, 'Putin's Trolls Are Targeting Trump's GOP Critics—Especially John McCain', *MotherJones.com*, 12 Jan 18. https://www.motherjones.com/politics/2018/01/putins-trolls-keep-targeting-john-mccain-and-other-gop-trump-critics/

[5] For the notorious example of Andrés Sepúlveda, who rigged elections in Latin America, using these types of methods, see 'How to Hack an Election', *Bloomberg*, 31 Mar 16. https://www.bloomberg.com/features/2016-how-to-hack-an-election/

[6] For Cambridge Analytica (as well as the views of its detractors, who suggest that the company has exaggerated the effectiveness of its methods), see Paul Wood, 'The British data-crunchers who say they helped Donald Trump to win', *The Spectator*, 3 Dec 16. https://www.spectator.co.uk/2016/12/the-british-data-crunchers-who-say-they-helped-donald-trump-to-win/ And also Nicholas Confessore and Danny Hakim, 'Data Firm says "Secret Sauce" aided Trump Campaign; Many Scoff', *The New York Times*, 6 Mar 17. https://www.nytimes.com/2017/03/06/us/politics/cambridge-analytica.html

subjugating the enemy. One text, very well-known and much discussed by military theorists, is the 1999 book *Unrestricted Warfare*, authored by two senior colonels from the Chinese Peoples' Liberation Army (PLA). They argued that in the face of American technological superiority, that non-kinetic actions might be more important to winning a conflict than weaponry. The key in future conflicts would be to employ asymmetric attacks on all elements of national power – economic, political, information, and military – as a mean to deter, intimidate, or defeat a militarily superior enemy. As the authors observed, "nothing is off the table."[7]

But who are the individual players at the heart of asymmetric (and specifically information) warfare doctrine? Generally speaking, powers using these techniques deploy a range of tactics - information warfare, which combines intelligence, counterintelligence, disinformation, subversion through proxies, and psychological pressure. Given the sheer range of stratagems, actors attempting to undermine societies through disinformation or influence operations need not necessarily use an organized cadre of specialists. Russian sources have from time to time also indicated that they posses "information troops, but this has been a widely misunderstood term.[8] As Russian military expert and Head of the Center for Military Forecasting, Anatoly Tsyganok, has observed, "the personnel of the Information Troops should be composed of diplomats, experts, journalists, writers, publicists, translators, operators, communications personnel, web designers, hackers, and others..."[9]

Major powers such as Russia and China have the ability to get their netizens to do the bidding of the state with very little nudging or recompense. In Russia's cyber conflicts with Estonia in 2007 and Georgia in 2008 (the latter conflict

[7] Qiao Liang and Wang Xiang Sui, *Unrestricted Warfare*, PLA Literature and Arts Publishing House, Beijing, February 1999. For an excerpt and summary translation see https://fas.org/nuke/guide/china/doctrine/unresw1.htm

[8] For a general overview of Russian information warfare, see Keir Giles, '"Information Troops" – A Russian Cyber Command?', July 2011, https://www.researchgate.net/profile/Keir_Giles/publication/224247775_Information_Troops__A_Russian_Cyber_Command/links/55b6514a08ae9289a08abd4e/Information-Troops-A-Russian-Cyber-Command.pdf

[9] BBC Monitoring: "Russia is underestimating information resources and losing out to the West", *Novyy Region*, 29 October 2008.

also having a real-world element), it was noticeable that sections of the Russian online community were keen to assist the Kremlin by pitting their hacking skills against the adversary. Likewise with actors in the information/disinformation space. Often, these are people who are willing to help, or be co-opted, with sometimes little or not reimbursement. One expert from a western European country told the present author that disinformation in his country was carried out by not more than 10 individual with pronounced right wing sympathies living in Moscow – some, according to him, were paid but others felt a strong ideological impetus – they felt that their country had gone down the wrong path (when it came to multiculturalism, and in terms of its immigration and refugee policy) and felt that they and the fake social media accounts they had created will aid in the "legitimate" resistance that would bring their country to the "correct" path again.

Consider, too, what is known of the Chinese "Internet army" also known as the "50cent army", which fabricates by some estimates over 400 million social media comments annually. These posts engage broadly in internet activism, drowning out negative comments on China and Beijing's policies on a variety of issues, putting also a positive sheen on various issues where this suits Beijing's interests. [10] The studies that exist on the subject suggest that while some components of the "50cent Army" might have links to the PLA, many are either individual netizens or institutions seemingly far removed from the information warfare space. One study of Chinese information warfare militias found that of 50 units analyzed, 18 were in fact associated with educational institutions.[11]

Legal Regimes – and International Rules of the Road (?)

It is clear that governments worldwide will need to create and enforce

[10] Gary King, Jennifer Pan, and Margaret E.Roberts, 'How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, not Engaged Argument', 14 Jan 17. *American Political Science Review*, (2017), 111 (3), pp.484-501. https://gking.harvard.edu/files/gking/files/how_the_chinese_government_fabricates_social_media_posts_for_strategic_distraction_not_engaged_argument.pdf

[11] For discussion, see R Shelon and J McReynolds, "Civil Military Integration and Cybersecurity: A Study of Chinese Information Warfare Militias", In *China and Cybersecurity : Espionage, Strategy and Politics in the Digital Domain*, ed. JR Lindsay et al (NY : OUP, 2015). http://oxfordindex.oup.com/view/10.1093/acprof:oso/9780190201265.003.0008

safeguards. There are various legislatives moves afoot worldwide (subject of a separate paper to be sent by RSIS researchers to the Parliamentary Select Committee). Some of these concern attempts to bring the major social media platforms to heel when it comes to accountability (for example, when it comes to removing hate speech within stipulated time limits). [12] The full import of these measures and their effectiveness will take some time to be seen. It will be a challenge for Governments to deal with the issue while ensuring that there is no government overreach. In the view of the present writer, laws to prevent the spread of fake news in Germany and France (which is mulling such a law) are likely to be highly politicized affairs, running up against traditional, and deeply held protections for the freedom of speech.

Separately, there has from time to time been discussion on some sort of international set of norms or basic understandings on controlling various issues in the cyber and disinformation spheres - akin to a Geneva Convention on these subjects. At present, these attempts appear to have failed for the time being, and it appears extremely unlikely that nations will attempt at any point in the near future to come together to talk over red lines and rules of the road when it comes to disinformation campaigns. One difficulty with this is that in kinetic (armed) warfare, deterrence can be effective as actors involved are prepared to display their force. However, in the disinformation space (as well as more generally in cyber), deterrence may not be effective as state actors are not prepared to show the arsenal of tools they have at their disposal. Concomitantly, the actors involved do not show what their "red lines" are where the threshold that might invite retaliation has been breached.

The status quo means that in terms of fomenting instability in targets countries, from the point of view of the aggressor, nothing is off the table and there are no norms. This ambiguity leaves room for escalation on the part of the aggressor. On the part of the targeted country, it is also difficult to take action against fake news/disinformation campaigns as it is not always clear (or not made clear in a timely fashion) who the adversary is. The powers sought by any government contemplating legislation tend to be broad. It is therefore not a simple matter to justify these powers to the public, which may not fully

[12] For the German example, see Zoey Chong, 'Germany kicks year off with strict online hate speech law', *CNET*, 1 Jan 18. https://www.cnet.com/news/german-hate-speech-law-goes-into-effect-on-1-jan/

understand that state actors might be trying to undermine the resilience of a country which has enjoyed a steady state of normalcy over decades.

Singapore: Implications & Recommendations

Any nation operating on a democratic model with regular elections and an open internet regime should be watching carefully the techniques and tactics tried by powers that have tried to influence and undermine society in countries such as the United States and in Europe. But beyond this, what is urgently required is serious study of 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. An aggressor could attempt to "peel off" one particular ethnic group or religion, using social media and disinformation to appeal (as the case may be) to deeply ingrained historical, cultural issues, setting off one group against others, or even against the government. Singapore can be a sandbox for subversion.

It should be observed, too, that countermeasures against disinformation should not be concerned solely with threats emanating from afar. There is evidence that some of these techniques are being used in some of Singapore's near neighbours. Data-driven political consultancies (whose methods may involve disinformation) appear to have been engaged by political parties, as well as individual candidates, in the coming Malaysian general election. [13]

In Indonesia, the use of political disinformation and organized spreading of smears through social media has become commonplace. One notorious Indonesian fake news factory, Saracen, charged customers for spreading fake news, and is thought to have been involved in spreading rumours against the former governor of Jakarta, Basuki Tjahaja Purnama (including attacks against

[13] There are reports that Cambridge Analytica numbers in their ranks. Boo Suu-Lyn, 'How Malaysian Politicians Use Big data to Profile You', *The Malay Mail Online*, 10 April 17. http://www.themalaymailonline.com/malaysia/article/how-malaysian-politicians-use-big-data-to-profile-you#9o5H8M5Wf5d8zwRm.97 ; Boo Suu-Lyn, 'Big Data' Firm Denies Doing Election Work in Malaysia, *Malay Mail Online*, 26 Mar 17. http://www.themalaymailonline.com/malaysia/article/big-data-firm-denies-doing-election-work-in-malaysia

his Chinese ancestry and his Christian religion), popularly known as "Ahok."[14] One administrator of Saracen was in January 2018 sentenced to jail for "intentionally spreading information to incite hate" on social media.[15] Online fake news factories have also for some time now been targeting President Joko Widodo, claiming that he is a Chinese Christian in cahoots with China.[16] It seems unlikely that Indonesia will be able to successfully tackle its fake news problem in the foreseeable future, partly on account of the lucrative nature of the business. One estimate suggested that one single popular post on Saracen could rake in Rp 100 million ($7,500 USD) because of the wide reach of the site.

Recommendations

This section provides suggestions for the continuum of non-legislative measures that should complement any proposed law dealing with fake news/disinformation.

Try the new…

Researchers from with whom the present writer has interacted (Ukraine, the Baltics, and other states facing disinformation on a daily basis) have intimated that shoring up trust between people and government is key. The citizenry should be taken into confidence and the nature of the threat to cohesion should be clearly laid out, without fear-mongering. Because of this underlying trust, their citizens are less disposed to believe fake news.

[14] 'Indonesia court sentences administrator of 'fake news factory' Saracen to jail', *The Straits Times*, 12 Jan 2018. http://www.straitstimes.com/asia/se-asia/indonesia-court-sentences-administrator-of-fake-news-factory-saracen-to-jail

[15] The individual in question was charged for violating the Electronic Information and Transactions Law. Rizal Harahap, 'Court sentences Saracen member to 32 months in prison', *The Jakarta Post*, 12 Jan 18. http://www.thejakartapost.com/news/2018/01/12/court-sentences-saracen-member-to-32-months-in-prison.html

[16] Adi Renaldi, 'Saracen in Shut Down. But can we ever really Beat Fake News?', *Vice.com*, 26 Aug 17. https://www.vice.com/en_id/article/3kk7v5/saracen-has-been-shut-down-but-can-we-ever-really-beat-fake-news

But even as government builds trust, the responsibility of combatting fake news and disinformation should not solely lie with the authorities. 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, disclosing the disinformation campaign substance and the vehicles, and systematically building social resilience.

In some countries, the best anti-disinformation websites and portals are run by citizens, journalists, or a coalition of both. In many instances, it is the citizenry and journalists (as well as media experts, branding experts, and marketing consultants) who are better placed to act, and to act quickly, to combat disinformation. Ukraine's *Stopfake.org*, which positions itself as public service journalism, is a crowdsourced journalism project that launched in 2014 to combat fake news spreading across the Internet during Ukraine's crisis in Crimea. The widely-respected site provides fact checking, verifies information, and refutes incorrect reports and propaganda about events in Crimea, which are widely believed to originate from Russia. [17] In Indonesia, the volunteer-run *Turn Back Hoax*, which has been online since 2016, has grown into an important resource for Indonesians to check the veracity of memes and fake stories.[18]

- Singapore could consider establishing a body – not necessarily a government one – that uses grassroots participation to counter fake news and disinformation operations. This institution could (1) carry out research and fact-checking initiatives, and congregate various experts under its umbrella to wage targeted campaigns against fake news (particularly when organized fake news campaigns are brought to bear against the people); (2) produce content for TV, newspapers and social media to debunk fake news and inform audiences, and (3) offer training to media professionals and other relevant parties.

[17] For the work done by Stopfake and its methods, see Andrew E.Kramer, 'To Battle Fake News, Ukrainian Show Features Nothing but Lies', The New York Times, 26 Feb 17. https://www.nytimes.com/2017/02/26/world/europe/ukraine-kiev-fake-news.html

[18] Adi Renaldi, 'Saracen is Shut Down. But can We Ever Really Beat Fake News?', *Vice.com*, 26 Aug 17. https://www.vice.com/en_id/article/3kk7v5/saracen-has-been-shut-down-but-can-we-ever-really-beat-fake-news

- NATO has a Centre of Excellence (COE) for Hybrid Threats located in Riga, Latvia. The NATO COE is well respected by practitioners and academics working in the field of disinformation. While the NATO model centers on a specific concern (Russia), there is some merit in studying the COE model with the view of introducing countermeasures customised to Southeast Asia's cultural and political landscape. Singapore should consider setting up a comparable Centre of Excellence for hybrid threats and disinformation – this would be a first in Southeast Asia. As ASEAN Chair in 2018, and with cyber (and by implication issues relating to social media) on its stated agenda for its chairmanship, Singapore would be well-positioned to promote concrete efforts.

- A smart nation needs a wise citizenry. There is an urgent need to cultivate critical thinking skills upstream – skills that will empower students to think intelligently and in an informed fashion when dealing with information and news. The Organisation for Economic Co-operation and Development's (OECD) Director for Education has called for children to be taught in schools how to spot fake news, with the suggesting that such skills will be included as measurable in the next round of PISA tests. [19] The Ministry of Education in Singapore is making some efforts in this regard, but more should be done. Critical thinking skills fostered from a young age make it more likely that the citizenry of Singapore's SMART Nation will in future have the underlying resilience to recognize filter bubbles and echo chambers of the mind.

And revisit the old…

- Revisit and review Total Defence - especially the critical psychological pillar of Total Defence. Various countries (particularly those in northern Europe) which have their own form of Total Defence have in the last 10-15 years revisited their own concepts, in part-recognition that threats are likely to come not just from big-ticket, kinetic attacks, but from slow burn issues (such as disinformation and also cyber threats),

[19] Sean Coughlan, 'Schools Should Teach Pupils How to Spot "Fake News"', *BBC*, 18 March 2017, http://www.bbc.com/news/education-39272841

too. The point of some of these revisions is to make for a more resilient society, and (in some cases) to emphasize the importance of civil-military cooperation, rather than separating these into different silos.

- The present writer suggests that ways should be found to support The Straits Times and Lianhe Zaobao, in a nuanced and calibrated fashion, such that they can once again be seen as the pre-eminent news sources, bar none, in the eyes of the Singapore public. While numerous amateur blogs and forums which have sprung up which to some degree provide commentary over Singapore-related issues, their coverage is patchy and none of these platforms can be considered a serious, consistent news source in the mould of The Straits Times and Lianhe Zaobao.

Even as governments clamp down on fake news through legislation, fact-checking websites and NGOs that put out correctives, the actors behind fake news appear to be calibrating their methods. They are beginning to evolve their methods in ingenious ways - *telling fewer lies and more truth*, with the same objectives and possibly even more success, using slant, interpretation, or weasel words. The fake news/disinformation threat is thus changing, with subtler – but equally effective – methods being deployed. Cooperation across the public and private sectors as well as media and civil society will be necessary when it comes to devising countermeasures. These countermeasures must in turn go hand in hand with efforts to shoring up resilience and a national consensus. This is painstaking work that will require constant tending. As one commentator observes, "It is easy to manufacture a lie, and relatively cheap to distribute it widely. To demolish that lie takes intensive effort, and meanwhile the nature of the internet ensures that it lives, breeds and reinforces other lies." [20]

--o0o--

[20] Keir Giles, Russia's 'New' Tools for Confronting the West : Continuity and Innovation in Moscow's Exercise of Power, Chatham House Research Paper, March 2016, p.51. https://www.chathamhouse.org/sites/files/chathamhouse/publications/2016-03-russia-new-tools-giles.pdf

Suggestions for further reading:

Who Said What? The Security Challenges of Modern Disinformation Highlights from the Workshop. Report. Canadian Security Intelligence Service. February 2018. https://csis.gc.ca/pblctns/wrldwtch/2018/2018-02-22/disinformation_post-report_eng.pdf.

Marwick, Alice , and Rebecca Lewis. *Media Manipulation and Disinformation Online.* Report. Data and Society Research Institute. https://datasociety.net/pubs/oh/DataAndSociety_MediaManipulationAndDisinformationOnline.pdf.

Bentzen, Naja. *Disinformation, 'fake news' and the EU's response.* European Parliamentary Research Service. http://www.europarl.europa.eu/RegData/etudes/ATAG/2017/608805/EPRS_ATA(2017)608805_EN.pdf.

Jakub Janda, and Ondřej Kundra. *Mechanisms of Influence of the Russian Federation into Internal Affairs of the Czech Republic.* Report. European Values Think-Tank. September 04, 2016. http://www.europeanvalues.net/wp-content/uploads/2016/09/Mechanisms-Of-Influence-Of-The-Russian-Federation-Into-Internal-Affairs-Of-The-Czech-Republic.pdf.

Norman Vasu, Benjamin Ang, Terri-Anne-Teo, Shashi Jayakumar, Muhammad Faizal, and Juhi Ahuja, 'Fake News : National Security in the Post-Truth Era', RSIS Policy Report, January 2018. https://www.rsis.edu.sg/wp-content/uploads/2018/01/PR180119_Fake-News-National-Security-in-Post-Truth-Era.pdf