Written Representation 135

Name: Benjamin Ang
Senior Fellow / Coordinator Cyber and Homeland Defence, Centre of Excellence for National Security (CENS), S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University

Received: 7 March 2018

Lies, Laws, and Legitimacy

Written submission to the Select Committee on Deliberate Online Falsehoods

Submitted by Benjamin Ang

1 Introduction

This paper is written in response to the invitation by the Select Committee on Deliberate Online Falsehoods – Causes, Consequences and Countermeasures, to submit written representations on any matter falling within the Terms of Reference, specifically:

> 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.

The author adopts the position in the Green Paper titled "Deliberate Online Falsehoods: Challenges and Implications" issued by the Ministry of Communications and Information and the Ministry of Law, which recognizes that deliberate online falsehoods are being spread worldwide to attack public institutions and individuals, with the aim "to sow discord amongst racial and religious communities, exploit fault-lines, undermine public institutions, interfere in elections as well as other democratic processes, and weaken countries." (Ministry of Communications and Information and the Ministry of Law , 2018)

1.1 Scope and Scale

This paper focuses on deliberate online falsehoods that amount to **national security threats**, originating from state or non-state actors who wish to destabilize Singapore. These will include '**information operations**', a term used in this paper to describe "integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making." (United States Air Force, 2006)

The tools for information operations can work synergistically or independently. They can include conventional intelligence operations, cyberattacks, disinformation operations, leveraging on political allies, agents of influence and non-governmental organizations (NGOs) in the targeted country, support for local extremists and fringe groups as well as disenfranchised ethnic minorities, and economic operations with political goals. (Jayakumar, 2017)

2 Existing and Proposed Legislation

States have had to deal with disinformation and propaganda for time immemorial. This is a brief look at some existing and proposed legislation that are relevant.

2.1 Singapore

The Sedition Act prohibits activity with a tendency to bring the government or the courts into hatred or contempt, raise discontent and disaffection among the citizens of Singapore, or create hostility between different races and classes of people in Singapore. Courts can prohibit the circulation of seditious publications. This has been used, inter alia, against local bloggers who posted seditious messages.

Under the **Broadcasting Act**, a broadcasting license can be suspended or cancelled if there has been a contravention of the license, any relevant Code of Practice, or the directions of the Minister or the MDA.

The **Films Act** makes it an offence to make distribute or exhibit a party political film, i.e. one which is made by any person and directed towards any political end in Singapore, such as matters intended or likely to affect voting in an election in Singapore, or contains biased references or comments on political matters including elections, candidates, issues before electors, the government or a previous government or opposition, a current government policy, or a political party. Films such as *Singapore Rebel, Zahari's 17 Years and Lim Hock Siew*, have all been banned in Singapore.

The Internal Security Act prohibits publications that compromise national interests, public order and security, and have a subversive tendency i.e. contains incitement to violence, encourages disobedience to the law, calculated or likely to lead to promote feelings of hostility between different races of classes of population, or is prejudicial to national security.

Under **Defamation Law,** a person who has been the subject of a defamatory statement, can sue if he/she was identified, the statement lowered his/her reputation, and it was published to at least one other person.

2.2 Europe

The German Network Enforcement Act imposes fines on social media companies up to 50 million euros (US$53 million) if they fail to remove 'obviously illegal' content (e.g. hate speech, defamation and incitements to violence) within 24 hours of receiving a complaint. (Grigonis, 2017)

The Italian Senate in February 2017 considered a Bill to require individuals who wish to open "an online platform aimed at publishing or disseminating information to the public" to notify the territorial tribunal via certified email, and provide the name of the platform, URL, name and surname of the administrator and tax number. (Fanucci, 2018)

France's President Emmanuel Macron announced in January 2018 that he would introduce a law requiring websites to make public the identity of those who sponsor content on their websites and will cap the amount of sponsored content. Emergency procedures could be introduced during elections to allow judges to remove content, close user accounts, or block websites that publish false information during these periods (Keohane, 2018)

2.3 USA

The Foreign Agents Registration Act (FARA) was used against Russian media channel RT, requiring them to "make periodic public disclosure of their relationship with the foreign principal, as well as activities, receipts and disbursements in support of those activities." (The U.S. Department of Justice, 2018) The US is also considering passing the Honest Ads Act, which targets foreign nationals and seeks to prevent "contributions, expenditures, and disbursements for electioneering communications… in the form of online advertising." (S.1989 – Honest Ads Act: 115th Congress (2017-2018), 2018)

2.4 Philippines

The Philippines Senate is considering a Bill imposing fines of P100, 000 (US$1,950) to P5 million (US$97,587) and 1 to 5 years of imprisonment for people guilty of creating or distributing fake news. (Senate of the Philippines 17th Congress, 2018)

3 Limitations of Legislation

Laws serve an important role in maintaining political and social order (Tan & Chan, 2017). However, while domestic laws can be effective against criminals, they are often not the correct tools for responding to state level attacks.

3.1 Multi-prong, Strategic Nature of Information Operations

When deliberate online falsehoods are used as part of Information Operations, they are only the tip of the iceberg. Legislation that penalizes or takes down online content (Germany, France, Philippines) can be circumvented by any of these other channels:

1. State sponsored media of foreign countries (e.g. RT, CCTV)

2. Business organisations or clan associations, especially if their members have business in foreign countries
3. Non-Government Organisations that have been infiltrated
4. Political parties that share the same views, or that have been infiltrated
5. Academics (e.g. Prof Huang Jing who had his permanent residency revoked for being an agent of influence)
6. Deceptive websites, designed to look like mainstream news (e.g. ABCnews.com.co; cnn-trending.com)
7. Extreme or biased websites (Breitbart.com, Infowars.com)
8. Computational propaganda / bots on social media – software designed to mimic human activity online, to create illusion of huge support for a specific view (e.g. those used by Russia during the US Presidential Election Campaign 2016)
9. Organised teams of civilians (e.g. China's '50 cent army')
10. Volunteer groups of civilians (e.g. China's 'Bring your own grainers')

Information operations can work on "slow-burn issues that can be equally, if not more, pernicious." (Jayakumar, 2017). As part of a larger, long term strategy, the deliberate online falsehood may be a decoy, distraction, or ruse. The operation of law can even be manipulated strategically by the attacker.

For example, extreme or deceptive websites can post a series of stories about a sensitive topic (e.g. immigration, elections, taxes) in Country X, that range from total falsehood, to half-truths, to biased reporting, to stories that appear to be false but are later shown to be true (e.g. through leaked information). Organised or volunteer groups of civilians share these stories on social media platforms that can be read in country X. In response, the Government of Country X uses its laws to compel the social media platforms to take down some or all the stories, and compels local ISPs to block the original websites.

Foreign state-sponsored media then reports that these stories have been taken down, displaying screen shots of the original stories, and highlighting the elements of truth (or half-truth) in some of the stories, with the headline "What is Country X hiding?"

Businessmen, NGOs, politicians, academics, and others in Country X who are part of the operation, share screen shots of the stories in private chat groups, together with the narrative that the Government is supressing the truth. Large numbers of social media users, and/or automated bots, share and re-share the stories in different forms, on different platforms, in discussion groups and in comment threads, also sharing the narrative that the Government is suppressing the truth.

In this scenario, when the Government of Country X uses the law to take down the deliberate online falsehoods, it has played into the hands of the attacker, who uses it to feed the conspiracy theory and sow doubt. X may have won the legal battle but is losing the war for trust and legitimacy.

3.2 Conspiracy Theories and Backfire Effect of Corrections

Alternatively, instead of taking down the story, the Government may want a right to respond to deliberate online falsehood, compelling platforms to publish an official correction. This assumes that the platforms will find a way to make the corrections visible alongside the falsehoods and any variants.

However, official responses can also result in the 'backfire effect', where corrections increase misperceptions among the target group, because it threatens their worldview. (Nyhan & Reifler, 2006) This is because conspiracy theories arise because of fundamental aspects of human psychology – our tendency to find patterns, seek meaning and subconsciously embrace biases in systematic ways. (Brotherton, 2017)

For example, China's aggressive efforts to censor social media posts, have instead reinforced some users' belief that the censored posts are true, while dismissing officially sanctioned newspapers as government propaganda. (Zeng, Chan, King-Wah, & Sutcliffe, 2017) In this state, these users are more likely to seek and trust news from alternative sources than from official sources.

3.3 Difficulty of Attribution

In the scenario above, the Government of Country X could take action under sedition laws, internal security laws, or defamation law, if the originators are persons or organizations in their jurisdiction. However, it would not be able to arrest foreign social media users, anonymous users, automated bots, or anyone else outside its shores.

3.4 Perceptions and Legitimacy

This gap has led countries like Germany to focus their laws on the social media platforms instead. However, this in turn can create problems of perception and legitimacy.

> Some German legal experts argue that the law on fake news violates Article 5 of the German constitution, which guarantees the freedom of expression and the right to information. This is especially because social media platforms are pro-actively taking down news (Rohleder, 2018)
>
> French opposition politicians, responding to President Macron's plans to pass legislation against fake news, warn that "only authoritarian regimes claim to control the truth." (Serhan, 2018)

In other nations, some political leaders have labelled their critics as “fake news”:

> Philippine President Duterte has banned local news site Rappler, which has published articles critical of his administration, from covering his events, accusing them of being “fake news”. Advocacy groups have argued that this is an attempt to intimidate independent journalists and to stifle valid criticism. (Mogato, 2018)
>
> US President Donald Trump constantly accuses his critics in the media of peddling “fake news”, but he has in turn been accused of doing so in bad faith, deliberately using such accusations to “addle the concentration of casual readers and viewers.” (Shafer, 2018)

This has led to fears that legislation against online falsehoods can be misused to suppress criticism and to erode freedom of speech. Legitimacy in the exercise of power is much greater when it is limited, and not left to any authority’s unfettered discretion. This is helped by transparency in decision making and meaningful checks and balances. (Feintuck & Varney, 2006)

Checks and balances can come from

(1) Creating a judicial process to execute the law (which can be expedited if needed), and/or
(2) Creating an independent multi-stakeholder body to review decisions

This independent body, if constituted as a multi-disciplinary force, can also seek to identify if falsehoods are part of a larger information operation, and to respond strategically (not every story should be taken down or rebutted immediately) instead of reactively.

4 Principles to guide Singapore’s response

The policy report ‘Countering Fake News: A Survey of Recent Global Initiatives’ (Muhammad Faizal, Haciyakupoglu, Yang, Suguna, & Leong, 2018) was prepared by the Centre of Excellence for National Security (CENS), S. Rajaratnam School of International Studies (RSIS), NTU, and is attached as an Annex to this written submission. It examines key legislative approaches in different countries and recommends a multi-pronged approach as a more thorough means to combat fake news. This approach combines *pre-emptive*, *immediate*, and *long-term* measures as set out in the figure and summary below. More details can be found in the Annex.

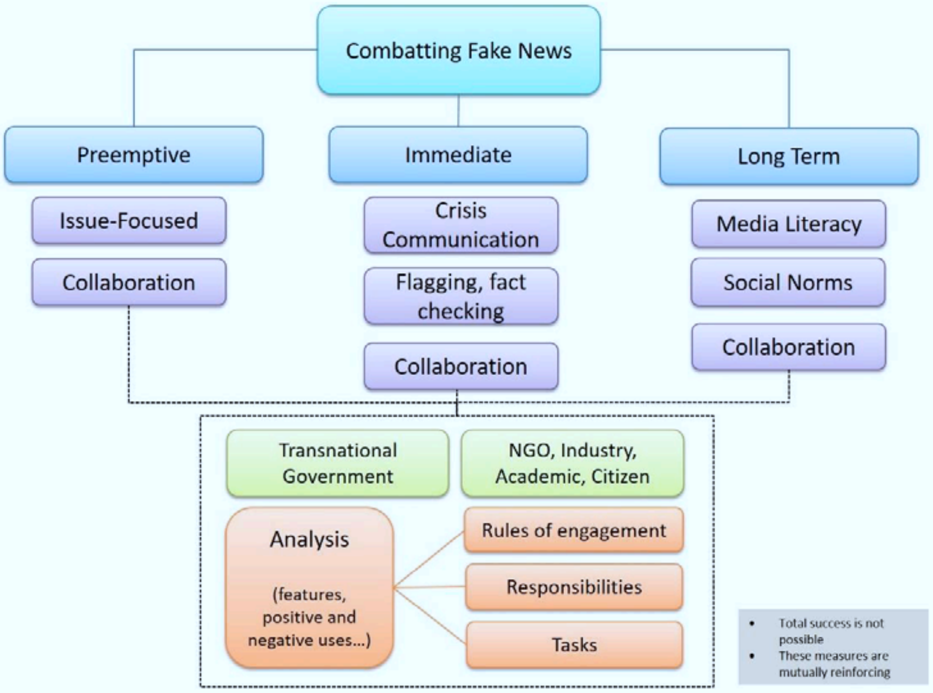

Figure 1: Multi-prong approach from 'Countering Fake News: A Survey of Recent Global Initiatives'

4.1 Summary

Pre-Emptive Measures (Before a campaign of deliberate online falsehoods is expected)	**Immediate Measures** (When a campaign has started)	**Long Term Measures**
Government collaborates with other stakeholders (social media companies, civil society, journalists; other countries) to target specific issues; Government conducts inter-agency crisis communication exercises.	Government issues transparent, timely, and accurate information; Independent fact checkers debunk the falsehoods; Social media users flag the items as false	Build media literacy in the population; Encourage social norms against sharing information without checking; Define the responsibilities of technology companies

4.2 Implementing the Multi-Prong Approach

For the immediate measures to be effective, there must be an environment of trust, which is built, in the pre-emptive stage, on continuous, transparent communication between public and government. The Latvian approach to building social resilience to falsehoods (Berzins, 2017) is a useful model:

1. Explain and identify the problem, and the attackers' tactics, to the public
2. Implement national level strategic communications to win hearts and minds, and minimize the gap between government and citizens
3. Enhance critical thinking through education, and
4. Engage citizens directly without media (face to face)

During the immediate measures phase, drawing parallels with work in countering violent extremism (CVE), credible non-government voices are often more effective than official messaging, especially with face-to-face contact. (Jayakumar, 2017) These credible voices could be community leaders or trusted public figures, or even trusted business entities.

In the longer term, because information operations are transnational attacks on one's society, the society needs to form its own norms, while the international or regional community also needs to develop norms of behaviour and even international law to regulate such operations.

5 Recommendations

1. Set up a multi-stakeholder multi-disciplinary organisation to implement the multi-prong approach described above.
2. Establish a process for the organisation to examine whether individual deliberate online falsehoods are part of larger information operations, and respond strategically.
3. Build in explicit checks and balances into any legislation dealing with deliberate online falsehoods, such as judicial processes and right of appeal to the courts or an independent body.
4. Establish timelines for relevant laws to be reviewed to deal with changing tactics.
5. Encourage norms against spreading deliberate online falsehoods locally and seek to build cooperation for regional or international norms or international law in the long term.

The author is willing to appear before the Committee to give evidence, if required.

Benjamin Ang,
March 2018

6 References

Berzins, J. (2017). Integrating Resilience in Defence Planning against Information Warfare. *APPSNO 2017.* Singapore: RSIS.

Bezanson, R. P. (2003). *How Free Can The Press Be?* Illinois: University of Illinois.

Brotherton, R. (2017). Suspicious Minds: Psychology of Conspiracy Theories. *Distortions Rumours Untruths Misinformation Smears.* Singapore: RSIS.

Chua, M. H. (1 Feb, 2018). *Has trust in the government been eroded?* Retrieved from The Straits Times: http://www.straitstimes.com/opinion/forging-trust-by-engaging-those-who-feel-it-has-waned

Fanucci, F. (1 Feb, 2018). *How Italy wants to slam fake news: Use fines and prisons.* Retrieved from Media Power Monitor: http://mediapowermonitor.com/content/how-italy-wants-slam-fake-news-use-fines-and-prison

Feintuck, M., & Varney, M. (2006). *Media Regulation Public Interest and the Law.* Edinburgh: Edinburgh University Press.

Grigonis, H. (30 June, 2017). *Delete hate speech or lose millions, the German Network Enforcement Act says.* Retrieved from Digital Trends: https://www.digitaltrends.com/social-media/network-enforcement-act-germany

Jayakumar, S. (14 August, 2017). Disinformation: Slow Burn Menace. *RSIS Commentaries.*

Keohane, D. (4 January , 2018). *Macron announces bill to tackle spread of fake news.* Retrieved from Financial TImes: https://www.ft.com/content/4ad6aed8-1f57-3985-8990-136e5e9ef075

Ministry of Communications and Information and the Ministry of Law . (5 January, 2018). *Annexe A: Green Paper.* Retrieved from Ministry of Law: https://www.mlaw.gov.sg/content/minlaw/en/news/press-releases/select-committee-deliberate-online-falsehoods.html

Mogato, M. (20 February, 2018). *Philippine leader bans news site from covering his events.* Retrieved from Reuters: https://www.reuters.com/article/us-philippines-media/philippine-leader-bans-news-site-from-covering-his-events-over-fake-news-idUSKCN1G41UN

Muhammad Faizal, A. R., Haciyakupoglu, G., Yang, J., Suguna, V. S., & Leong, D. (2018). *Countering Fake News - A Survey of Recent Global Initiatives.* Singapore: RSIS.

Nyhan, B., & Reifler, J. (2006). When Corrections Fail: The Persistence of Political Misperception. *Political Behaviour.*

Pearson, M. (2007). *The Journalist's Guide to Media Law.* Australia: Allen & Unwin.

Rohleder, B. (20 Feb, 2018). *Germany set out to delete hate speech online. Instead, it made things worse.* Retrieved from Washington Post: https://www.washingtonpost.com/news/theworldpost/wp/2018/02/20/

S.1989 – Honest Ads Act: 115th Congress (2017-2018). (1 Feb , 2018). Retrieved from Congress.gov: https://www.congress.gov/bill/115th-congress/senate-bill/1989

Senate of the Philippines 17th Congress. (1 Feb, 2018). *Senate Bill 1492: Anti Fake News Act of 2017.* Retrieved from Senate of the Philippines 17th Congress: https://www.senate.gov.ph/lis/bill_res.aspx?congress=17&q=SBN-1492

Serhan, Y. (6 Jan, 2018). *Macron's War on Fake News.* Retrieved from The Atlantic: https://www.theatlantic.com/international/archive/2018/01/macrons-war-on-fake-news/549788/

Shafer, J. (19 January, 2018). *Donald Trump's fake news mistake.* Retrieved from Politico: https://www.politico.eu/blogs/on-media/2018/01/donald-trumps-fake-news-mistake/

Tan, E., & Chan, G. (2017). *The Singapore Legal System.* Retrieved from Singaporelaw.sg: http://www.singaporelaw.sg/sglaw/laws-of-singapore/overview/chapter-1

The U.S. Department of Justice. (1 Feb, 2018). *Foreign Agents Registration Act (FARA).* Retrieved from The U.S. Department of Justice: https://www.fara.gov/.

United States Air Force. (2006). *What are information operations".* Retrieved from Air University: http://www.au.af.mil/info-ops/what.htm.

Zeng, J., Chan, C.-h., King-Wah, F., & Sutcliffe, D. (3 October , 2017). *Censorship or rumour management? How Weibo constructs "truth" around crisis events .* Retrieved from The Policy and Internet blog: http://blogs.oii.ox.ac.uk/policy/censorship-or-rumour-manage

Countering Fake News: A Survey of Recent Global Initiatives

By Muhammad Faizal bin Abdul Rahman, Gulizar Haciyakupoglu, Jennifer Yang Hui, V S Suguna and Dymples Leong[1]

Executive Summary

Governments worldwide are taking various steps to tackle the scourge of fake news which may be driven by different motivations but most onerous are those that serve as a tool for disinformation; i.e. to undermine national security. Key among these steps is the introduction of new legislation:

- New laws that are being proposed or have been passed would give governments more powers to hold technology companies (e.g. Facebook, Twitter and Google) and individuals accountable for the spread of fake news.

- Laws would also seek to counter the impact of automated social media accounts (bots). In response, technology companies have intensified efforts to defend themselves and are enhancing capabilities to detect and remove fake news.

- At present, it is too early the gauge the impact of legislation.

Legislation however would face certain challenges and thus should be complemented by a continuum of non-legislative measures including:

- Pre-emptive measures that are focused on an issue (i.e. elections) and supplemented by continuous collaborative engagements with the industry, non-governmental sector and regional fora;

- Immediate measures that comprise an agile crisis communications plan and fact-checking initiatives; and

- Long-term measures that strengthen social resilience through media literacy, inculcation of social norms on responsible information sharing, and defining the responsibilities of technology companies.

Going forward, a multi-pronged strategy that comprises both legislation and non-legislative measures – given that each have their challenges - would form a more sustainable bulwark against fake news.

[1] *Muhammad Faizal bin Abdul Rahman and Gulizar Haciyakupoglu are Research Fellows, Jennifer Yang Hui and V S Suguna are Associate Research Fellows, and Dymples Leong is Senior Analyst at the Centre of Excellence for National Security (CENS), a constituent unit of the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University, Singapore.*

Contents

1. Introduction

Fake news, while not a novel phenomenon,[2] has seized global attention in the wake of the U.S. presidential election in 2016. Fake news in the digital era span a spectrum of categories, with varied but at times overlapping motivations: political, subversive, financial and entertainment.[3] The impact of fake news is amplified through: (a) internet platforms, which publish content with significantly lower cost, wider reach and rapid circulation; (b) social media, which enables more people and groups of various persuasions to interact even as they consume, produce and re-circulate content; and (c) artificial intelligence (AI) agents that automate the work of human propagators. The term "fake news" is also used by parties to denigrate content or points of view at odds with their own beliefs.[4]

Fake news becomes a national security issue when it undermines the foundations (e.g. social cohesion, public institutions, peace and order) of the nation state. In this regard, fake news could serve as a tool for disinformation campaigns: the intentional dissemination of false information for influencing opinions or policies of the receiving audience.[5] An example is the revelation that Russian operatives have uploaded socially and politically divisive social media content to influence the outcome of the 2016 U.S. Presidential election.[6] A notable case in Singapore is the conviction of a couple in 2016 for operating a seditious website (The Real Singapore) that generated advertising revenue by propagating falsehoods that fuelled xenophobia.[7]

Unsurprisingly, researchers and policymakers worldwide have sought not just to understand the phenomenon, but to develop strategies, including new laws, to curb its spread.

[2] Before the advent of the Internet, the phenomenon was seen as propaganda in which the mass media had been a vehicle for propaganda that was exploited by both state and non-state actors to push messages that distort the opinions and emotions of people largely for the promotion of certain political agenda or ideology.

[3] "Infographic: Beyond Fake News – 10 Types of Misleading News," *European Association for Viewers Interest (EAVI)*, accessed November 7, 2017, https://eavi.eu/beyond-fake-news-10-types-misleading-info/.

[4] James Carson, "What is fake news? Its origins and how it grew in 2016," *The Telegraph*, March 16, 2017, http://www.telegraph.co.uk/technology/0/fake-news-origins-grew-2016/.

[5] Naja Bentzen, "Understanding disinformation and fake news," *European Parliament Think Tank*, accessed November 7, 2017, http://www.europarl.europa.eu/RegData/etudes/ATAG/2017/599408/EPRS_ATA(2017)599408_EN.pdf.

[6] "Russia-linked posts reached 126m Facebook users in US," *BBC*, October 31, 2017, http://www.bbc.com/news/world-us-canada-41812369.

[7] Pearl Lee, "TRS co-founder Yang Kaiheng jailed 8 months for sedition," *The Straits Times*, June 28, 2016, http://www.straitstimes.com/singapore/courts-crime/trs-co-founder-yang-kaiheng-jailed-8-months-for-sedition.

2. Legislating Fake News: Global Case Studies[8]

COUNTRY	LEGISLATION	
	STATUS	ACCOUNTABLE PARTY
Germany	Approved	Technology companies
Italy	Pending	Individuals, website administrators, Internet Service Providers (ISP), schools
The Philippines	Pending	Individuals and technology companies
Russia	Pending	Technology companies
U.S.A.	Pending	Technology companies
	Pending	Technology companies
U.K.	Pending	Technology companies
Australia	In progress	Technology companies, online advertisers and other parties who benefit from disinformation.
Israel	Pending	Technology companies
India	Approved	Administrators of social media groups
Canada	In action	Mass media

Table 1: Fake news legislation worldwide

Some countries see legislation as being the best approach to tackle the problem of fake news. In the legislation proposals, accountability is mostly placed on technology companies, but also individuals. New technological dynamics are also taken into account by the proposals.

2.1 Legislative Proposals

2.1.1 Accountable Party: Technology companies

Many of the proposed legislation hold technology companies accountable for the dissemination of fake news, call for faster removal of offending content, and recommend steep fines, even imprisonment, for failure to contain fake news dissemination. The German Network Enforcement Act, for instance, imposes fines on social media companies in a sum of as much as 50 million euros (US$53 million) if they fail to remove 'obviously illegal' content (e.g. hate speech, defamation and incitements to violence) within 24 hours upon receiving a complaint.[9] For offensive online material that requires further assessment, the Act compels companies to block the offending content within seven days, failing which a fine will be imposed.

[8] See Appendix A.

[9] Hillary Grigonis, "Delete hate speech or lose millions, the German Network Enforcement Act says," *Digital Trends*, June 30, 2017, accessed 10 November 2017, https://www.digitaltrends.com/social-media/network-enforcement-act-germany/.

2.1.1.i Responses from Technology companies

Technology companies have been intensifying efforts to combat fake news. Facebook, in addition to enhancing machine learning and increasing its efforts to remove accounts,[10] pledged to add more than 1,000 people to its global ads review teams over the next year to inspect political ad purchases. Twitter has vowed to increase the precision of algorithmic tools to combat disinformation.[11] The micro-blogging platform has also promised to update its community guidelines.[12] Under the new measures, Twitter users will be able to see details such as the types of ads targeted, ad duration, ad spend, the identity of organisations and the demographics targeted by the ads. Google planned to release its election ad transparency report in 2018, and provide its database to public for future research. Facebook, Google and Twitter appeared in court on October 31 and November 1, 2017 to defend their role during the 2016 U.S. presidential election.

2.1.1.i.a. US Congressional Hearing: Testimonies by Technology Companies

During the Senate hearings in November 2017, Facebook, Twitter and Google responded to questions on the role of technology companies during the 2016 election. Investigations revealed that Russian-linked entities such as the Internet Research Agency (IRA) used fake accounts on social media platforms to create content which undermined the election process. Fake accounts were used to purchase ads and post politically divisive content in attempts to sow discord online. Facebook, for instance, has since estimated that Russian content had reached about 126 million Americans on its platform.[13]

Intense scrutiny has been directed at technology companies for their failure to identify Russian-linked fake accounts. In response, Twitter provided the steps taken during its internal investigations at identifying and removing Russian-linked accounts. Russian-linked accounts that were active between 1 September and 15 November 2016 were removed if they met any of the following criteria: (1) the accounts utilised Russian email addresses, mobile numbers or credit cards; (2) Russia was the declared country on the account; or (3) Russian language or Cyrillic characters appeared in the account information or name.[14] While Google

[10] Colin Stretch, "Hearing before the United States Senate Committee on the Judiciary Subcommittee on Crime and Terrorism – Testimony of Colin Stretch, General Counsel, Facebook," *Committee on the Judiciary,* October 31, 2017, https://www.judiciary.senate.gov/imo/media/doc/10-31-17%20Watts%20Testimony.pdf.

[11] Kent Walker, "House Permanent Select Committee on Intelligence Russia Investigative Task Force Hearing with Social Media Companies," *United States House of Representatives Permanent Select Committee*, November 01, 2017, https://intelligence.house.gov/uploadedfiles/prepared_testimony_of_kent_walker_from_google.pdf.

[12] Sean Edgett, "U.S. Senate Committee on the Judiciary: Opening Remarks," *Twitter Blog*, October 31, 2017. https://blog.twitter.com/official/en_us/topics/company/2017/opening_remarks.html.

[13] Mike Isaac and Daisuke Wakabayashi, "Russian influence reached 126 million through Facebook alone," *The New York Times*, October 30, 2017, https://www.nytimes.com/2017/10/30/technology/facebook-google-russia.html.

[14] Sean Edgett, "United States House of Representatives Permanent Select Committee on Intelligence – Testimony of Sean J. Edgett, Acting General Counsel, Twitter, Inc," *United States House of Representatives Permanent Select Committee*, November 1, 2017, accessed November 16, 2017, https://intelligence.house.gov/uploadedfiles/prepared_testimony_of_sean_j._edgett_from_twitter.pdf.

found activities associated with suspected government-backed accounts of Russian origin, it stated that these activities had been minimal. Due to the limited capability to target audiences on a micro-level, the company argued that there were fewer cases of interference than alleged.[15]

Technology companies have also taken pains to emphasise their efforts in countering fake news. For example, Twitter announced on 26 October 2017 – prior to the US Congressional hearings – its decision to ban Russian news outlets such as Russia Today (RT) from advertising on its platform.[16] Following the Senate hearings, the US government compelled RT to register with the Foreign Agents Registration Act (FARA) of 1938, which required individuals acting as agents of foreign influence with the capability to influence the government or public to "make periodic public disclosure of their relationship with the foreign principal, as well as activities, receipts and disbursements in support of those activities."[17] In a measure similar to FARA, Russia recently announced that it will require all foreign news agencies operating in the country to be registered as 'foreign agents.'[18]

2.1.1.i.b. Honest Ads Act

Technology companies are troubled over the proposed Honest Ads Act, a bipartisan US Senate bill aiming to regulate online political advertising. The bill, if passed, will compel companies to disclose details such as advertising spending, targeting strategies, buyers and funding. It will also subject online political campaigns to adhere to stringent disclosure conditions for advertising on traditional media. Proponents claim such disclosures would result in added transparency towards online political advertising. Technology companies have highlighted their efforts towards self-regulation such as the voluntary contributions as well as the commitment towards fighting foreign interference and disinformation on their platforms.

2.1.1.i.c. National Defense Authorisation Act (NDAA)

The U.S. NDAA of 2017 approved the establishment of Global Engagement Center to "lead, synchronise, and coordinate" Federal Government's efforts to "counter foreign state and non-state propaganda and disinformation efforts aimed at

[15] Kent Walker. "House Permanent Select Committee on Intelligence Russia Investigative Task Force Hearing with Social Media Companies," *United States House of Representatives Permanent Select Committee*, November 1, 2017, https://intelligence.house.gov/uploadedfiles/prepared_testimony_of_kent_walker_from_google.pdf

[16] Dominic Rushe, "Twitter bans ads from RT and Sputnik over election interference," *The Guardian*, October 26, 2017.

[17] "Foreign Agents Registration Act (FARA)," *The U.S. Department of Justice*, accessed November 28, 2017, https://www.fara.gov/.

[18] Thomas M. Hill, "Is the U.S. serious about countering Russia's information war on democracies?," Brookings, November 21, 2017, https://www.brookings.edu/blog/order-from-chaos/2017/11/21/is-the-u-s-serious-about-countering-russias-information-war-on-democracies/.

undermining United States national security interests."[19] The center has been instrumental in responding to the Islamic State of Iraq and the Levant's (ISIL) 'messaging.'[20] The 2018 version of NDAA, which was passed by Congress in July 2017, has gone a step further and proposed several actions that specifically target Russian disinformation operations. Some of its proposed actions include "joint, regional, and combined information operations and strategic communication strategies to counter Russian Federation information warfare," instalment of interagency measures to manage and implement strategies against disinformation operations of Russia and further collaboration with NATO Strategic Communications Center of Excellence (NATO StratCom COE).[21] The NATO StratCom COE, established in 2014, regards strategic communication as an important apparatus in realising military and political aims, and aspires to support friendly-forces' strategic communication processes through offering analysis, 'timely advice', and practical aid.[22] Through the declaration of its interest to further engage with NATO Stratcom COE, the U.S. has signalled its acknowledgement of the importance of international collaboration in countering disinformation operations.

2.1.2. Accountable Party: Individuals

Some legislation proposals recommend tough penalties for individuals found responsible for disseminating false content. In the Philippines, for instance, the proposed Senate Bill No. 1492 threaten those guilty of creating or distributing fake news with a fine ranging from P100, 000 (US$1,950) to P5 million (US$97,587) and 1 to 5 years of imprisonment.[23] If the offender is a public official, fine and period of imprisonment will be doubled. Offenders will be disqualified from holding any public office. Other recommended actions include regulatory measures such as identity management in registration of online domains. A legislative bill submitted to the Italian Senate in February 2017 require individuals who wish to open "an online platform aimed at publishing or disseminating information to the public" to notify the territorial tribunal via certified email, and provide the name of the platform, URL, name and surname of the administrator and tax number.[24]

[19] "S.2943 – National Defense Authorization Act for Fiscal Year 2017," *Congress.Gov*, accessed November 27, 2017, https://www.congress.gov/bill/114th-congress/senate-bill/2943/text.

[20] "Global Engagement Center," *U.S. Department of State: Diplomacy in Action*, accessed November 29, 2017, https://www.state.gov/r/gec/.

[21] "H.R.2810 - National Defense Authorization Act for Fiscal Year 2018," *Congres.Gov*, accessed November 27, 2017, https://www.congress.gov/bill/115th-congress/house-bill/2810/text

[22] "About us," *NATO StratCom Centre of Excellence*, accessed November 29, 2017, https://www.stratcomcoe.org/about-us.

[23] "Senate Bill 1492: Anti Fake News Act of 2017," *Senate of the Philippines 17th Congress*, accessed November 10, 2017 at https://www.senate.gov.ph/lis/bill_res.aspx?congress=17&q=SBN-1492.

[24] Francesca Fanucci, "How Italy wants to slam fake news: Use fines and prisons," *Media Power Monitor,* 13 March 2017, http://mediapowermonitor.com/content/how-italy-wants-slam-fake-news-use-fines-and-prison.

2.1.3. New Technological Dynamics

New dynamics brought about by technological advancements is a concern for governments looking to legislation to combat fake news. Justice Ministers in three German states, for example, have proposed anti-botnet legislation to reduce the impact of automated social media accounts in disseminating fake news. Botnets - networks comprising of remotely controlled computers - are suspected to have engineered voter sentiments during recent events such as the United Kingdom European Union membership referendum and the 2016 U.S. elections. Jenna Abrams, a popular Twitter account that attracted up to 70,000 followers through its support for U.S. President Donald J. Trump and advocacy of far-right views, for example, is believed to have been run by the Russian propaganda machine for the purpose of discrediting the Democrats.[25] The role of automated accounts in influencing elections was raised during the U.S. Senate hearings as well.

2.1.4. Extraterritorial Legal Application

To date, most proposed legislation against fake news does not directly address the issue of extraterritorial application. However, some proposed bills do have extraterritorial implications. Germany's Network Enforcement Act mandated the establishment of a local point of contact for transnational technology companies to cooperate with local law enforcement authorities on takedown requests. The proposed Honest Ads Act, although framed generally in terms of protecting U.S. domestic order, targets the role of foreign nationals and seeks to prevent "contributions, expenditures, and disbursements for electioneering communications… in the form of online advertising."[26]

In summary, some governments are looking to legislation as a tool to manage the challenges of fake news. While many governments are determined to hold technology companies to account despite the latter's assertion of their ability for self-regulation, it is currently too early to assess the efficacy of current legislative provisions against fake news. While the efficacy of legislative measures against fake news is expected to be an on-going subject of study, as part of a holistic approach towards tackling fake news, governments around the world have also undertaken non-legislative initiatives to combat fake news.

2.2 Non-Legislative Measures

Legislation alone is insufficient in tackling the challenges of fake news. In recognition of this fact, some countries prefer to beef up the enforcement of existing legislation instead of introducing new ones. Others prefer implementing non-legislative measures.

[25] Caroline Mortimer, "Jenna Abram: Popular Far Right U.S. Twitter account revealed as a Russian Propaganda Outlet," *The Independent*, November 03, 2017, http://www.independent.co.uk/life-style/gadgets-and-tech/news/jenna-abrams-twitter-account-russia-propaganda-far-right-voice-alt-tweet-blog-xenophobic-donald-a8035411.html.

[26] "S.1989 – Honest Ads Act: 115th Congress (2017-2018)," *Congress.gov*, accessed November 23, 2017, https://www.congress.gov/bill/115th-congress/senate-bill/1989.

In Indonesia, online smear campaigns had affected electoral candidates' standing in national and regional elections since 2012. There are evidence that some of these politically-motivated smear campaigns have been aided by well-organised "fake news factories" such as the Saracen Cyber Team, an online-based syndicate that created many social media accounts to spread hate speech for clients willing to pay for them.[27] Online sectarian and racist narratives had polarised public opinion in the lead-up to the Jakarta gubernatorial elections in February and April 2017 that saw the defeat of former governor, Basuki Tjahaja Purnama, a Chinese Christian.[28] To deal with the problem of fake news, the Indonesian government has enforced existing legislation such as Article 156 and 156(a) of the Criminal Code (KUHP)[29] and in 2016 introduced new provisions to the Electronic Information and Transactions Act.[30] In 2015, the Indonesian National Police issued Circular SE/06/X/2015 to guide law enforcement in implementing existing legislation against hate speech.[31] In 2017, the police also formed the Multimedia Bureau to hunt for fake news in social media.[32]

In order to tackle the challenges of fake news in a more comprehensive manner, governments around the world are looking to non-legislative initiatives to tackle fake news.[33] Czech Republic, for instance, established the Centre Against Terrorism and Hybrid Threats to tackle non-traditional challenges such as disinformation campaigns.[34] Non-legislative initiatives also include fact-checking and counter fake news websites. Malaysia, for example, introduced an information verification website (sebenarnya.my) to counter fake news.[35] Meanwhile, Qatar launched the 'Lift the Blockade' website to fight disinformation campaigns and provide its own perspective.[36] Other non-legislative programs aim to inculcate media literacy and critical thinking. Countries such as Canada, Italy and Taiwan are introducing school curriculum that teaches children to discern

[27] Wahyudi Soeriaatmadja, "Indonesian police probe alleged fake news factory's protest links," *The Straits Times*, August 26, 2017, http://www.straitstimes.com/asia/se-asia/indonesian-police-probe-alleged-fake-news-factorys-protest-links.

[28] Merlyna Lim, "Beyond fake news: social media and market-driven political campaigns," *The Conversation*, September 05, 2017, https://theconversation.com/beyond-fake-news-social-media-and-market-driven-political-campaigns-78346.

[29] Irfan Abubakar, "Managing hate speech or muzzling freedom of expression?," *Indonesia at Melbourne*, November 20, 2015, http://indonesiaatmelbourne.unimelb.edu.au/surat-edaran-hate-speech-freedom-expression/.

[30] Kristo Molina, "Indonesian Electronic Information and Transactions Law Amended," *White & Case*, December 15, 2016, https://www.whitecase.com/publications/alert/indonesian-electronic-information-and-transactions-law-amended

[31] Azyumardi Azra, "Hate Speech and Freedom," *Republika*, November 05, 2015, http://www.republika.co.id/berita/en/resonance/15/11/05/nxc6o1317-hate-speech-and-freedom. See also Abubakar, "Managing hate speech or muzzling freedom of expression?".

[32] Farouk Arnaz, "National Police Form New Unit to Tackle 'Fake News' on Social Media," *Jakarta Globe*, February 22, 2017, http://jakartaglobe.id/news/national-police-form-new-unit-to-tackle-fake-news-on-social-media/. See also Margareth S. Aritonang, "National Police to enlarge institution focusing on cybercrimes," *The Jakarta Post*, http://www.thejakartapost.com/news/2017/01/06/national-police-to-enlarge-institution-focusing-on-cybercrimes.html.

[33] See Appendix B.

[34] Robert Tait, "Czech Republic to fight 'fake news' with specialist unit," *The Guardian*, December 28, 2016, https://www.theguardian.com/media/2016/dec/28/czech-republic-to-fight-fake-news-with-specialist-unit

[35] Fairuz Mohd Shahar, "Communications Ministry launches sebenarnya.my to quash fake news, information," *New Straits Times*, March 14, 2017, https://www.nst.com.my/news/2017/03/220604/communications-ministry-launches-sebenarnyamy-quash-fake-news-information.

[36] Victoria Scott, "Qatar launches new website to counter 'fake news'," *Doha News*, September 19, 2017, https://dohanews.co/qatar-launches-new-website-to-counter-fake-news/. See also "Overview," *Lift the Blockage*, accessed November 22, 2017, https://lifttheblockade.com/overview/.

between false and credible information.[37] In addition, recognising the role of online opinion leaders, some country leaders such as Indonesian President Joko Widodo had also encouraged social media influencers to fight fake news by promoting unity.[38]

Governments are also funding research into using technology such as artificial intelligence (AI) and machine learning to address the challenges of fake news. The U.S. National Science Foundation has supported projects such as ClaimBuster, which uses national language processing techniques to spot factual claims within texts.[39] ClaimBuster has been used to check facts during the U.S. 2016 presidential election.[40] The software has also checked Hansard, the report of the proceedings of the Australian parliament and its committees, for possible false claims on a wide variety of issues of national interest such as budget and citizenship.[41]

[37] See Appendix B.

[38] "Jokowi tells social media influencers to step up fight against fake news", *The Jakarta Post*, August 24, 2017, http://www.thejakartapost.com/news/2017/08/24/jokowi-tells-social-media-influencers-to-step-up-fight-against-fake-news.html.

[39] ClaimBuster website, accessed November 23, 2017 at http://idir-server2.uta.edu/claimbuster/.

[40] "UTA researchers are refining their automated fact-checking system", *EurekAlert!*, August 24, 2017, accessed https://www.eurekalert.org/pub_releases/2017-08/uota-ura082417.php.

[41] Naeemul Hassan, et al, "ClaimBuster: The First-ever End-to-end Fact-checking System," *Proceedings of the VLDB Endowment* 10, No. 12 (2017): 1945-1948.

3. Recommendations

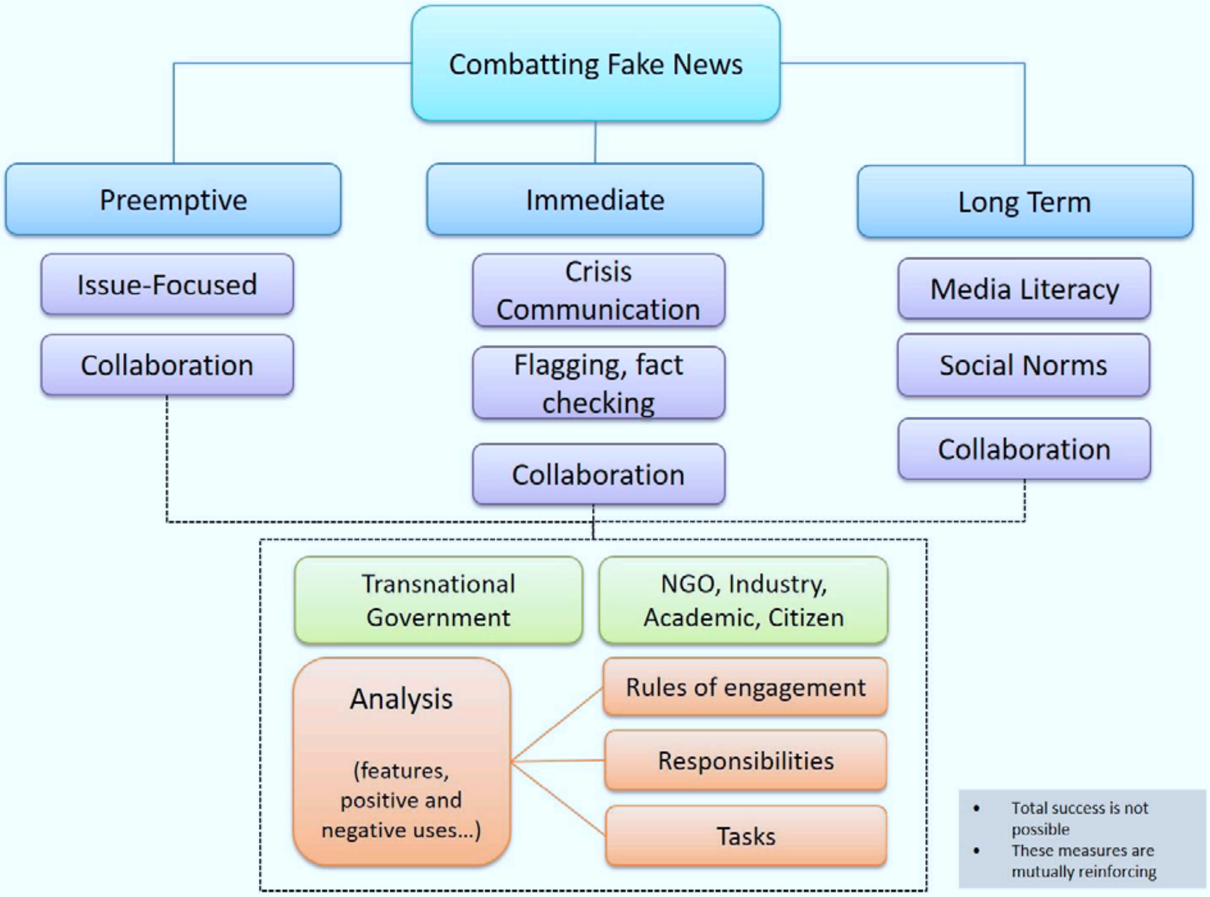

Figure 1: CENS multi-pronged framework for combatting fake news

Attempts to legislate fake news inevitably face challenges. Due to the speed and wide reach of information dissemination, as well as the ambiguity of what exactly constitutes fake news, using legislation to combat fake news is challenging. Legal measures to target fake news may result in unexpected scenarios: (1) Removing fake news may give rise to the so-called "Streisand effect", whereby deleting content increases audience attention on it. In China, for example, aggressive efforts to censor social media posts that are not in line with the government's narrative reinforced some netizens' belief that the censored posts represent the true state of matter, while dismissing officially sanctioned newspapers as government propaganda.[42] In this state, netizens are more likely to seek and trust news from alternative sources than before; (2) With the prospect of hefty fines looming over them, social media companies are likely to err on the side of caution by aggressively removing posts, driving healthy discourse underground.

[42] Jing Zeng, Chung-hong Chan, King-Wah Fu and David Sutcliffe, "Censorship or rumour management? How Weibo constructs "truth" around crisis events," *The Policy and Internet blog*, October 03, 2017, http://blogs.oii.ox.ac.uk/policy/censorship-or-rumour-management-how-weibo-constructs-truth-around-crisis-events/.

Given the aforementioned challenges, a multi-pronged approach will provide a more thorough means to combat fake news. This approach combines pre-emptive, immediate as well as long-term measures as part of a broad framework in tackling the challenges of fake news.

3.1 Pre-Emptive Measures

Pre-emptive measures that are conducted in a collaborative manner to target the issue at hand should be taken against fake news. An issue-focused approach to combat fake news is formed for particular purposes such as elections. This allows targeted definition of fake news in a particular context, and thus expedites the identification of related fictitious information. Collaboration on the other hand, (1) facilitates the exchange of knowledge and skills; (2) narrows the gap between local and global; (3) helps identify overlapping concerns between different issues and contexts; and (4) allows the transmission of a consistent message. Issue-focused, collaborative measures aimed at preventing the spread of fake news would facilitate a prompt and lasting response, and they would yield better results than isolated efforts that lack focus.

In the recent French and German elections, for instance, collaborative efforts focused on the issue of elections helped raise awareness on the danger of fake news. The measures taken also obstructed the circulation of fictitious information to some extent. Before the German elections, Facebook had been assisting the government through cooperation with the German Federal Office for Information Security, educating political candidates on online security concerns, and launching a channel dedicated to the 'reports of election security and integrity issues.'[43] The social media giant also terminated 30,000 accounts in France[44] and provided its users with various online tools such as a guide for spotting fake news and finding out and comparing candidates' 'campaign promises' in the lead-up to the French elections.[45] The First Draft-led fact-checking initiatives of CrossCheck (France) and WahlCheck17 (Germany) were other examples of pre-emptive collaborative actions that focused on a particular issue; elections.[46]

3.1.1 Collaborative Engagements

Collaborations to combat fake news may be conducted via: (1) Regional engagements; (2) Non-governmental collaborative efforts; and (3) Government-industry partnerships.

3.1.1.i. Regional Collaborations: Combating Fake News in ASEAN

[43] Josh Constine, "11 ways Facebook tried to thwart election interference in Germany," *TechCrunch*, September 27, 2017, https://techcrunch.com/2017/09/27/facebook-election-interference/.

[44] Eric Auchard and Joseph Menn, "Facebook cracks down on 30,000 fake accounts in France," *Reuters*, April 14, 2017, https://www.reuters.com/article/us-france-security-facebook/facebook-cracks-down-on-30000-fake-accounts-in-france-idUSKBN17F25G.

[45] Marie Mawad, "French Election is Facebook's Fake News Litmus Test," *Bloomberg Technology*, April 27, 2017, https://www.bloomberg.com/news/articles/2017-04-27/france-is-facebook-s-fake-news-litmus-test-as-elections-near-end.

[46] See section 3.1.1.ii.

Fake news should be tackled through concurrent efforts at the regional and international fora to share experiences and collaborate in mutually acceptable areas. For Southeast Asian states (AMS), the roundtable in September 2017 by the ASEAN Ministers Responsible for Information (AMRI) has set the stage for regional collaboration.[47]

As the ASEAN Chair in 2018, Singapore will be well-positioned to promote concrete efforts. It is important for these efforts to facilitate joint research in the fake news phenomenon in order to develop effective countermeasures that consider not only what the message said, but also its presentation, author, format as well as context.[48]

Going forward, AMS could study the experiences of other regional blocs particularly the European Union (EU) which formed the EU East StratCom Taskforce in 2015 to counter Russia's disinformation campaigns.[49] The task force serves as a regional mechanism that enables collaboration with a wide network of government officials, experts, journalists and think tanks.[50] The task force's activities dovetail with the strategic communications activities of NATO (North Atlantic Treaty Organisation), which include countering the use of disinformation campaigns by Russia for its geopolitical goals (e.g. in Ukraine).[51]

While the EU's and NATO's models center on a specific concern (i.e. Russia), there are nonetheless merits in studying these models with the view of introducing similar strategies customised to Southeast Asia's cultural and political landscape. To avoid over-securitisation of fake news and in line with the AMRI meeting in September 2017, regional efforts to counter fake news could be subsumed under the actions plan of the ASEAN Socio-Cultural Community.

[47] "ASEAN to cooperate on fighting fake news in the region", *Association of Southeast Asian Nations (ASEAN)*, September 13, 2017, http://asean.org/asean-to-cooperate-on-fighting-fake-news-in-the-region/.

[48] Victoria L. Rubin, "Deception Detection and Rumor Debunking for Social Media," *The SAGE Handbook of Social Media Research Methods*, London (2017): 21, https://uk.sagepub.com/en-gb/eur/the-sage-handbook-ofsocial-media-research-methods/book245370.

[49] "Questions and Answers about the East StratCom Task Force," *European Union External Action*, November 8, 2017, https://eeas.europa.eu/headquarters/headquarters-homepage_en/2116/%20Questions%20and%20Answers%20about%20the%20East%20StratCom%20Task%20Force.

[50] "EU strategic communications with a view to counteracting propaganda," *European Parliament, Directorate-General for External Policies, Policy Department*, (May 2016): 16, http://www.europarl.europa.eu/thinktank/en/document.html?reference=EXPO_IDA(2016)578008.

[51] "Digital Hydra: Security Implications of False Information Online," *NATO Strategic Communications Centre of Excellence Riga, Latvia,* November 8, 2017, https://www.stratcomcoe.org/digital-hydra-security-implications-false-information-online.

3.1.1.ii Extra-Governmental Collaborations

Extra-governmental alliances have invested great effort in combating fake news and should form part of the framework for combatting fake news. 'StopFake,' for instance, is a multi-pronged initiative that was established in 2014 in Ukraine to counter Russian disinformation operations and assess the impact of fake news in Ukraine as well as other countries and regions.[52] 'StopFake' offers opinion pieces, detailed outlook on Russian disinformation operations, access to researches on the issue, guidance on verifying fake information, and videos debunking fake news, which are broadcasted on their site and in local TVs.[53] Another comprehensive initiative, First Draft, helped combat fake news during the French elections via CrossCheck[54] and during the German elections via WahlCheck17 (in partnership with Correctiv)[55]. First Draft provides instructions on information verification, and congregates academic institutions, technology companies (including Google, Twitter, and Facebook), newsrooms (including Reuters, BBC and NBC), human rights organizations and other willing institutions under its umbrella to wage a war against fake news.[56] The International Fact Checking Network on the other hand has been coordinating and training fact-checkers around the world.[57]

A multi-pronged framework against fake news can tap on extra-governmental initiatives' vast networks. The diversity of participants' skills and knowledge will aid in building credible narratives against fake news. Collaboration with extra-governmental initiatives will also provide quick response to disinformation campaigns as these initiatives will not be encumbered by bureaucratic demands.

3.1.1.iii Government-Industry Partnerships

Striking the right balance between security needs and combating fake news is expected to be an on-going challenge. This is because any attempt to compel technology companies to provide access to customer data (via legal or alternative means) will invariably be perceived negatively. This might dissuade technology companies from establishing subsidiaries in Singapore. Singapore, like Denmark,[58] could create a digital ambassador to engage with technology companies to determine how best to increase collaboration and minimise disputes.

[52] "About us," *StopFake.org*, accessed November 28, 2017, https://www.stopfake.org/en/about-us/.

[53] StopFake.org, accessed November 28, 2017, http://test.stopfake.org/en/.

[54] "Our Projects – CROSSCHECK," *First Draft*, accessed November 28, 2017, https://firstdraftnews.com/project/crosscheck/.

[55] Claire Wardle, "#WahlCheck17: Monitoring the German election," *First Draft*, September 1, 2017, https://firstdraftnews.com/wahlcheck17-correctiv/.

[56] "About," *First Draft*, accessed November 28, 2017, https://firstdraftnews.com/about/

[57] International Fact Checking Network has gathered and trained fact-checkers around the globe. It offers analysis on the impact of fact-checking since its establishment in 2015. See "Poynter is a Thought Leader," *Poynter*, accessed November 6, 2017, https://www.poynter.org/about-us/poynter-thought-leader.

[58] Robbie Gramer, "Denmark Creates the World's First Ever Digital Ambassador," *Foreign Policy*, 27 January 2017, accessed 27 March 2017, http://foreignpolicy.com/2017/01/27/denmark-creates-the-worlds-first-ever-digital-ambassador-technology-europe-diplomacy/.

3.2 Immediate Measures

On the immediate level, transparent, timely and accurate communication must be carried out in tandem with affected bodies to dispel confusing information. An agile crisis communication plan should be put in place to provide an immediate response to disinformation operations. Inter-agency scenario planning and mock crisis exercises must be conducted on a regular basis to ensure crisis communication plans stay up-to-date, providing government agencies with preparatory time that will lead to operational advantage. Other immediate measures include fake news flagging initiatives and fact-checking websites. Fake news flagging allow social media users and companies to tag fictitious information in order to alert other readers, while fact-checking websites debunk deceptive information. Both measures have proven timely and effective in signalling false content to others.

For immediate measures to be effective, an environment of trust must be fostered. There is a need to retain public trust through continuous, transparent communication with public on the government's part. Nevertheless, maintaining public trust, especially during times of conflicting information, will be challenging. In this case, communication may be carried by NGOs comprising of experts in the issues of interest. This would foster greater citizen trust in the information conveyed due to the impartiality of the communicating party. As an illustration, the Ukraine Crisis Media Center conducts 'daily briefings', 'roundtables' and 'discussions' to unpack complex information on Ukraine and beyond.[59]

3.3 Long-Term Measures: Media Literacy and Social Norms

Long term measures to combat fake news include: (1) Initiatives to inculcate media literacy. A number of countries such as Italy and Taiwan are already introducing media literacy in schools.[60] These efforts could be expanded to the elderly; (2) Encouraging social norms[61] against fake news such as responsible information sharing practices;[62] and (3) Defining the responsibilities of technology companies in countering fake news.

3.4 Legislating Fake News: A Silver Bullet?

It is currently too early to assess the negative and positive impacts of legislative initiatives against fake news, although these should be monitored. However, at this stage, it can be said that any

[59] "About Press Center," *Ukraine Crisis Media Center*, accessed November 28, 2017, http://uacrisis.org/about.

[60] The Italian government has partnered with technology companies such as Facebook to train students in recognising fake news. Taiwan schools are also planning to introduce curriculum to teach school children to develop critical thinking online.

[61] Social norms are one of the measures suggested for the regulation of the Internet. One example provided by Ang Peng Hwa (2007) is the exclusion of people who do not adhere to the group norms from online chat groups. See Ang Peng Hwa, "Framework for Regulating the Internet," in *The Internet and Governance in Asia: A Critical Reader*, ed. Indrajit Banjee (Asian Media Information and Communication Centre (AMIC) and Wee Kim Wee School of Communication and Information Nanyang Technological University (WKWSCI-NTU):2007, 328, 329, 330.

[62] Responsible information sharing practices include cross-checking, authenticating the source and the author as well as reading the information in full before sharing.

attempt to legislate against fake news will inevitably meet with difficulties given the (1) definitional issues with regards to what fake news entail; (2) global dimension of the cyberspace vis-à-vis the restriction of territorial boundaries of legislation; (3) challenges in identification of actual perpetrator of fake news and (4) sophistication of disinformation campaigns. Content-related regulations in cyberspace will also face obstacles. Firstly, it is important, yet difficult to 'reconcile' online regulations with offline regime.[63] For instance, while pornography is illegal in many Asian countries, it is challenging to regulate such content in cyberspace.[64] Secondly, variation in terms of what is legal and illegal in different countries[65] meant that "foreign undesirable materials"[66] may continue to be available in other countries despite one nation's efforts to outlaw it. It is therefore difficult to harmonise conflicting cultural values embedded in digital information content.[67] For example, hate sites blocked by Germany, may still be accessible in neighbouring European countries. These contents may also be accessible via virtual private network (VPN) despite Germany's efforts to restrict access to them.

Singapore has the necessary financial, educational and technological resources to adopt an approach that incorporates the abovementioned pre-emptive, immediate and long-term remedies, which provide a more comprehensive approach to tackling fake news. Moving forward, Singapore could consider establishing an impartial body devoted to the fight against disinformation operations. This institution could carry out research and fact-checking initiatives, congregate various experts under its umbrella to wage targeted war against fake news, as well as manage crisis communication specific to disinformation operations. The benefit of establishing such an organisation is that it can win the trust of citizens with its impartial stance, and help integrate citizens in the fight against fake news. The Singapore government should also increase efforts to elevate media literacy, explore the ways in which social norms can be established against the circulation of fake news, and expand collaboration with the technology companies, citizens, and other nations.

4. Conclusion

This report attempted to provide an overview of recent initiatives taken against fake news. While several countries are considering the use of legislation as a tool to manage the problem of fake news, it is currently at a nascent stage and therefore too early to assess the impact. It is thereby crucial to consider the implications in terms of possible challenges legislation may face before taking any action in this direction. In this respect, a multi-pronged strategy that incorporates pre-emptive issue-focused measures including collaborations with a wide variety of actors and organisations (regional organisations, NGOs and technology companies), immediate responses and long-term remedies such as media literacy and fostering social norms will be an appropriate approach going forward.

[63] Hwa, "Framework," 335.
[64] *Ibid*
[65] *Ibid.*
[66] *Ibid*, 338.
[67] *Ibid.*

Appendix A - Global Overview of Fake News Legislation

COUNTRY	LEGISLATION			TECH COMPANY RESPONSES
	STATUS	PRESCRIPTIVE ACTIONS	ACCOUNTABLE PARTY	
Germany	Approved	The Network Enforcement Act imposes fines on social media companies in a sum of as much as 50 million euros (US$53 million) if they fail to remove 'obviously illegal' content (such as hate speech, defamation and incitements to violence) within 24 hours upon receiving a complaint. For offensive online material that requires further assessment, action to block it must be taken by the companies within seven days, failing which a fine will be imposed. The Act does not appear to address extraterritorial application.	Technology companies	In May 2017, when the draft law was being announced, Facebook noted in a statement that while the company shared the German federal government's concern regarding hate speech and false news online, the Act is not a suitable tool to achieve these political goals. The Act would encourage social media companies to remove content that is not obviously illegal in the face of a "disproportionate threat of fines. It would in effect transfer responsibility for complex legal decisions from public authorities to private companies. Facebook has tested its tools for combating fake news during the 2017 German elections in response to government calls for more action. Facebook users could flag fake news and highlight them for review. Collaboration with fact-checking organisations such as Correctiv provides further information about disputed content. Google, along with Facebook, has also stepped up efforts to disrupt fake news.
	Pending	Anti-botnet legislation proposed by Justice Ministers in three German states (Hessen, Saxony-Anhalt and Bavaria) to deal with automated social media accounts that spread fake news.	Unknown	Facebook said that it does not have social bots on its platform, thanks to its real name policy and ban on fake profiles. Twitter insisted that the company strictly enforces its bot policies such as the banning of the automation of retweets and favouriting.

COUNTRY	LEGISLATION			TECH COMPANY RESPONSES
	STATUS	PRESCRIPTIVE ACTIONS	ACCOUNTABLE PARTY	
Italy	Pending	A legislative proposal was submitted on 7 February 2017 in the Senate of the Republic. The bill provides for the adoption of Article 656-bis of the Criminal Code. According to this provision, whoever publishes or circulates via the Internet fake news or exaggerated or biased information on manifestly ill-founded or false facts and circumstances shall be punished by a fine of up to EUR 5,000. Where the same conduct constitutes defamation, the aggrieved person may ask for the damages he/she actually suffered and seek additional pecuniary compensation. This provision only applies to online publications that are not registered as "online newspapers", in accordance with the criteria established by existing legislation, namely the Press Law no 47/148 and the Law on Publishing no 62/2001. As a result, only "non-journalistic" websites, blogs, and pages on social media would be punishable in case of publication of fake news.	Individuals	

COUNTRY	LEGISLATION			TECH COMPANY RESPONSES
	STATUS	PRESCRIPTIVE ACTIONS	ACCOUNTABLE PARTY	
		Additionally, the proposed bill introduces another criminal offence, namely Article 265-bis of the Criminal Code. According to this article, whoever circulates or communicates, including via the Internet, false, exaggerated or biased rumours or news likely to cause public alarm or threaten public interests in any way, or which may have a misleading impact on the public opinion, shall be punished by a fine of up to EUR 5,000.	Individuals	
		Further conduct that the proposed bill wishes to criminalise is contained in the new Article 256-ter of the Criminal Code. Under this provision, whoever carries out, including via the Internet, a hate speech campaign against certain individuals or against the democratic process shall be punished by at least two years' imprisonment and a fine of up to EUR 10,000.	Individuals	

COUNTRY	LEGISLATION			TECH COMPANY RESPONSES
	STATUS	PRESCRIPTIVE ACTIONS	ACCOUNTABLE PARTY	
		Anyone who wishes to open "an online platform aimed at publishing or disseminating information to the public" will have to notify the territorially competent tribunal via certified email, listing the name of the platform, the URL, the name and surname of the administrator and their tax number. The rationale of this norm is purportedly "to increase transparency and contrast anonymity" on the web.	Individuals	
		All the online platforms will have to publish, within 48 hours of receipt, the statements or rectifications sent by anyone who felt damaged by something published or who claims the information is false, as long as such statements are lawful. Failure to do so is punished with fines between €500 and €2,000.	Website administrators	

COUNTRY	LEGISLATION			TECH COMPANY RESPONSES
	STATUS	PRESCRIPTIVE ACTIONS	ACCOUNTABLE PARTY	
		Finally, the proposal also addresses the ISPs' obligations in respect of the activities and content posted by users. Pursuant to Article 7, ISPs must regularly monitor content, paying particular attention to any content that generates a substantial degree of interest among users, in order to assess the reliability and truthfulness of this content. In the event of an ISP determining that certain content does not meet this requirement, it must promptly remove the content in question; if the ISP fails to do so, it may be punished in accordance with Article 656-bis of the said Criminal Code.	Internet Service Providers (ISP)	
		Schools would also be bound by duty to teach students about 'media literacy' and 'citizen journalism' in order to protect them from fake news.	Schools	
		The proposed legislation does not appear to address extraterritorial application.		

COUNTRY	LEGISLATION			TECH COMPANY RESPONSES
	STATUS	PRESCRIPTIVE ACTIONS	ACCOUNTABLE PARTY	
The Philippines	Pending	A bill which seeks to penalize any person or group who maliciously spreads false news or information in traditional and online media platforms has been filed. The proposed Senate Bill No. 1492, entitled an "An Act Penalizing the Malicious Distribution of False News and Other Related Violations." It defines false news or information as "those which either intend to cause panic, division, chaos, violence, and hate, or those which exhibit a propaganda to blacken or discredit one's reputation." Under the bill, any person proven guilty of creating or distributing fake news will face a fine ranging from P100,000 to P5 million and 1 to 5 years of imprisonment. Violators who have aided and encouraged fake news meanwhile will be fined P50,000 to P3 million and imprisoned from 6 months to 3 years. If the offender is a public official, he will be made to pay twice the amount of fine and serve twice the period of imprisonment. He will also be disqualified from holding any public office. Mass media enterprise or social media platform that fails, neglects, or refuses to remove false news will be fined P10 million to P20 million and face 10 to 20 years of imprisonment. The proposed	Individuals and technology companies	

COUNTRY	LEGISLATION			TECH COMPANY RESPONSES
	STATUS	PRESCRIPTIVE ACTIONS	ACCOUNTABLE PARTY	
		bill does not address extraterritorial application.		

COUNTRY	LEGISLATION			TECH COMPANY RESPONSES
	STATUS	PRESCRIPTIVE ACTIONS	ACCOUNTABLE PARTY	
Russia	Pending	Two Russian lawmakers from State Duma majority party, United Russia, have proposed a bill for the publishing of “false information” on social media to become a criminal offence, punishable by hefty fines. If passed, the law would see individuals found to have violated the law face a fine of up to 5 million rubles ($83,000) and large corporations face a maximum penalty of 50 million rubles ($830,000). The proposed bill does not appear to address extraterritorial application.	One of the law's authors, Deputy Sergey Boyarsky, took to Twitter to assure critics that the law would target social media companies rather than individual users, stating that it would be “up to the organisers of information dissemination to delete illegal information”.	Russian social media companies have reacted negatively to the proposed bill. Vkontakte, a Russian-based social media platform, for instance, have pointed out that the proposed measures cannot contain the impact of false information and are impossible to implement.
United States of America (U.S.A.)	Pending	The Honest Ads Act, a bipartisan bill, was proposed by US Senators Amy Klobuchar, Mark Warner and John McCain. The proposed Senate bill, if approved and passed, would require internet companies to disclose details on political advertisements placed on the companies' platforms. Such details could include the buyer of political advertisements and the amount paid by the buyers for advertisements online. The proposed Act addressed extraterritorial application through seeking to prevent “contributions,	Technology companies	In the US Senate hearings in November 2017, representatives from Facebook, Google and Twitter were asked if they would support the approval of the bill. Without explicitly consenting to the conditions of the bill, representatives stated that technology companies would do all they can to tackle fake news.

COUNTRY	LEGISLATION			TECH COMPANY RESPONSES
	STATUS	PRESCRIPTIVE ACTIONS	ACCOUNTABLE PARTY	
		expenditures, and disbursements for electioneering communications by foreign nationals in the form of online advertising."		
	Pending	On-going proceedings by the US Federal Election Commission into paid fake news dissemination by Russia.	Technology companies	
United Kingdom (U.K.)	Pending	A Fake News Inquiry was convened in 2015 by the House of Commons Select Committee for Digital, Culture, Media and Sport Committee to understand the phenomenon of fake news and the impact of fake news on society, national security and democratic processes. In the aftermath of the 2016 UK referendum and the 2017 general election, the inquiry is focusing on obtaining written submissions from experts and members of the public pertaining to the role of foreign actors abusing online platforms to interfere in the political processes of the United Kingdom. It is currently unclear if the Inquiry will look into legislation.	Technology companies	The Committee has written to Facebook and Twitter requesting for details of advertising by Russian-linked accounts.

COUNTRY	LEGISLATION			TECH COMPANY RESPONSES
	STATUS	PRESCRIPTIVE ACTIONS	ACCOUNTABLE PARTY	
Australia	In progress	The Australian Parliament is establishing a "Select Committee on the Future of Public Interest Journalism" to examine the impact of fake news and countermeasures. This includes studying if legislation is necessary to counter fake news.	Technology companies, online advertisers and other parties who benefit from disinformation.	For the public hearing on 22 Aug 2017, Google and Facebook had made a submission which includes actions undertaken to address fake news.
Israel	Pending	In January 2017, the Israeli Knesset passed the first reading of a new bill that would allow the Israeli Administrative Affairs courts to order social media companies to remove online content that is considered incitement to violence. The proposed bill does not address extraterritorial application.	Technology companies	Following a September 2016 meeting in Israel, Facebook has said that it does not tolerate terrorism and agreed to create joint teams to tackle the problems of Internet incitement. The social media company has also said that it is working hard to remove problematic content within the shortest time possible. It also hopes to continue a "constructive dialogue" with Israel that discusses the "implications of this bill for Israeli democracy, freedom of speech, the open Internet and the dynamism of the Israeli Internet sector."
India	Approved	The Varanasi district magistrate issued a joint order stating that a first investigation report can be filed against a social media group's administrator if fake news are found to be circulating on his/her social media group. In the event of the group admin's inaction, he/ she will be considered guilty and action will be taken against him/her. The false post must be reported to the nearest police station so that action can be taken against the member under the law. The joint order does not address extraterritorial	Administrators of social media groups	

COUNTRY	LEGISLATION			TECH COMPANY RESPONSES
	STATUS	PRESCRIPTIVE ACTIONS	ACCOUNTABLE PARTY	
		application.		
Canada	Implemented	In October 2017, the Canadian Radio-Television and Telecommunications Commissions (CRTC) withdrew a proposal to revoke a rule on "prohibited programming content", which includes the broadcast of fake news. The rule does not address extraterritorial application.	Mass media	

Appendix B - Government-Initiated Measures against Fake News

COUNTRY	STATUS	ACTIONS
Qatar	Implemented	The Qatari government has launched a new website called “Lift the Blockade” to counter “fake news” amid the on-going Gulf crisis.
Malaysia	Pending	The Malaysian government has proposed making online websites (with high volumes of web traffic) to register with the Malaysian Communications and Multimedia Commission (MCMC).
	Implemented	The Malaysian Communications and Multimedia Commission (MCMC) has set up a website (Sebenarnya or "actually" in Malay) to counter fake news. The website caters to Malay-speaking audience and aims to debunk inaccurate news that appear on social media.
Czech Republic	Implemented	In Jan 2017, the Ministry of Interior created a specialist unit named Centre for Combating Terrorism and Hybrid Threats to counter disinformation that threaten national security. Social media platforms such as Twitter will be utilised in its operations. A new section of the interior ministry website will also be dedicated to communicating the views of the government. The centre will also train civil servants to avoid blackmail and resist foreign lobbying.
Indonesia	Implemented	Enforcement of existing legislation such as Article 156 of the Criminal Code (KUHP) and the 2008 Law regarding Information and Electronic Transaction. In 2015, the Indonesian National Police issued Circular SE/06/X/2015 to guide the law enforcement in operational management for managing hate speech. The Police have also formed a unit, named Multimedia Bureau, to monitor social media for misinformation. Its mandate includes disseminating information related to public order as well as educating users on pro-social usage of social media. The Indonesian Communications Ministry had also blocked websites that are found to disseminate hate speech. Recognising the role of online opinion leaders, Indonesian President Joko Widodo had also encouraged social media influencers to fight fake news through promoting unity.
Taiwan	In progress	In April 2017, the Executive Yuan and the National Communications Commission announced that they are looking to establish a cooperative relationship with Facebook and other social media platforms to establish fact-checking mechanism. The Taiwanese government is also using vTaiwan, an online tool to involve citizens in exchanging views on how to fight against disinformation.
Italy	In progress	The Italian government is partnering with Facebook and Google to teach students across 8,000 high schools to recognise fake information.
Sweden	In progress	In an effort to provide print media firms competitive advantage, the Swedish government has proposed to do away with tax on ad revenue for daily newspapers and periodicals. From July 2018 onwards, the Swedish school

COUNTRY	STATUS	ACTIONS
		curriculum will also teach students how to discern reliable and unreliable sources.
Finland	Implemented	The Finnish government has hired U.S. consultants to train Finnish officials in recognising and responding to fake news. Students are also taught to read news critically in schools.
China	Implemented	The Chinese military launched a website in November 2017 for the public to report leaks, fake news and illegal online activities by military personnel.
Canada	Implemented	NewsWise is an initiative to equip Canadian students aged nine to 19 in news literacy.
U.S.A.	Implemented	The National Science Foundation has supported projects such as ClaimBuster, which uses national language processing techniques to spot factual claims within texts. ClaimBuster has been used to check facts during the U.S. 2016 presidential election and 2017 Australian Parliament discussion on topics of national interest such as budget and citizenship.