Policy Report

COUNTERING FAKE NEWS
A SURVEY OF RECENT GLOBAL INITIATIVES

Gulizar Haciyakupoglu, Jennifer Yang Hui, V. S. Suguna, Dymphles Leong, and Muhammad Faizal Bin Abdul Rahman
March 2018
## Table of Contents

Executive Summary 3

Introduction 4

Legislating Fake News: Global Case Studies 5
  Legislative proposals 5
    Accountable party: technology companies
    Responses from technology companies
    US congressional hearing: testimonies by technology companies
    Honest ads act
    National Defense Authorisation Act (NDAA)
    Accountable party: individuals
    New technological dynamics
    Extraterritorial legal application
  Non-legislative measures 11

Recommendations 13
  Pre-emptive measures 15
    Collaborative engagements
    Regional collaborations: combating fake news in ASEAN
    Extra-governmental collaborations
    Government-industry partnerships
    Immediate measures
    Long-term measures: media literacy and social norms
  Legislating fake news: a silver bullet? 20

Conclusion 22

Appendix A 23

Appendix B 31

About the Authors 33

About the Centre of Excellence for National Security 35

About the S. Rajaratnam School of International Studies 35
Executive Summary

Governments worldwide are taking various steps to counter 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. Not only that, certain challenges might be faced and legislation 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 forums;

• 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.
Introduction

Fake news, while not a novel phenomenon, has seized global attention in the wake of the US 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. The impact of fake news is amplified through: (i) internet platforms, which publish content with significantly lower cost, wider reach, and faster circulation; (ii) social media, which enables more people and groups of various persuasions to interact even as they consume, produce, and re-circulate content; and (iii) 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.

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. An example is the revelation that Russian operatives did actually upload socially and politically divisive social media content to influence the outcome of the 2016 US Presidential election. 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. Unsurprisingly, researchers and policymakers worldwide have sought not just to understand the phenomenon, but also to develop strategies, including new laws, to curb its spread.

1 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.
Legislating Fake News: Global Case Studies

Table 1: Fake news legislation worldwide (as at January 2018)

<table>
<thead>
<tr>
<th>Country</th>
<th>Legislation</th>
<th>Accountable party</th>
</tr>
</thead>
<tbody>
<tr>
<td>Germany</td>
<td>Approved</td>
<td>Technology companies</td>
</tr>
<tr>
<td>Italy</td>
<td>Pending</td>
<td>Individuals, website administrators, Internet Service Providers (ISP), schools</td>
</tr>
<tr>
<td>The Philippines</td>
<td>Pending</td>
<td>Individuals and technology companies</td>
</tr>
<tr>
<td>Russia</td>
<td>Pending</td>
<td>Technology companies</td>
</tr>
<tr>
<td>USA</td>
<td>Pending</td>
<td>Technology companies</td>
</tr>
<tr>
<td></td>
<td>Pending</td>
<td>Technology companies</td>
</tr>
<tr>
<td>UK</td>
<td>Pending</td>
<td>Technology companies</td>
</tr>
<tr>
<td>Australia</td>
<td>In progress</td>
<td>Technology companies, online advertisers and other parties who benefit from disinformation.</td>
</tr>
<tr>
<td>Israel</td>
<td>Pending</td>
<td>Technology companies</td>
</tr>
<tr>
<td>India</td>
<td>Approved</td>
<td>Administrators of social media groups</td>
</tr>
<tr>
<td>Canada</td>
<td>In action</td>
<td>Mass media</td>
</tr>
</tbody>
</table>

Legislative proposals

Some countries see legislation as being the best approach to counter 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.

Accountable party: technology companies

Several proposed legislation hold technology companies accountable for the dissemination of fake news, call for faster removal of offending content,

7 See Appendix A.
and recommend steep fines and imprisonment for failure to contain fake news dissemination. The German Network Enforcement Act, for instance, imposes fines as much as 50 million euros (US$53 million) on social media companies if they fail to remove “obviously illegal” content within 24 hours upon receiving a complaint. 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.

**Responses from technology companies**

Technology companies have been intensifying efforts to combat fake news. Facebook, in addition to enhancing machine learning and increasing efforts to remove accounts, 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. The micro-blogging platform has also promised to update its community guidelines. 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 plans 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 31 October and 1 November 2017 to defend their roles during the 2016 US presidential election.

---


US congressional hearing: testimonies by technology companies

During the Senate hearings in November 2017, Facebook, Twitter, and Google responded to how their platforms were used as a tool for interference in the 2016 election. Investigations revealed that Russian-linked entities such as the Internet Research Agency used fake social media accounts to create content, undermining the election process. Fake accounts were used to purchase ads and post politically divisive content in attempts to sow discord online. Facebook, for instance, estimated that Russian content had reached about 126 million Americans on its platform.12

Intense scrutiny has been directed at technology companies for their failure to identify Russian-linked fake accounts. In response, Twitter explained the steps taken during its internal investigations at identifying and removing such accounts.13 While Google 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.14

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.15

---


13 Twitter had removed Russian-linked accounts that were active between 1 September and 15 November 2016 if they met any of the following criteria: (i) the accounts utilised Russian email addresses, mobile numbers or credit cards; (ii) Russia was the declared country on the account; or (iii) Russian language or Cyrillic characters appeared in the account information or name. See 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.


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.”16 In a measure similar to FARA, Russia recently announced that it would require all foreign news agencies operating in the country to be registered as “foreign agents.”17

**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 would also require 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 -- new policies requiring political advertisers to disclose the identity of their organisations and campaigns -- as well as the commitment towards fighting foreign interference and disinformation on their platforms.

**National Defense Authorisation Act (NDAA)**

The US NDAA of 2017 approved the establishment of the Global Engagement Center to “lead, synchronise, and coordinate” the Federal Government’s efforts to “counter foreign state and non-state propaganda and disinformation efforts aimed at undermining United States national

security interests.” The Center has been instrumental in responding to the Islamic State of Iraq and the Levant’s (ISIL) “messaging.”

The 2018 version of NDAA, which was passed by Congress in July 2017, had gone a step further to propose 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 the North Atlantic Treaty Organisation Strategic Communications Center of Excellence (NATO StratCom COE).

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. Through the declaration of its interest to further engage with NATO Stratcom COE, the US has acknowledged the importance of international collaboration in countering disinformation operations.

**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 threatens 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 one to five years

---

If the offender is a public official, fine and period of imprisonment will be doubled. Offenders will also be disqualified from holding 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, web address, name and surname of the administrator, and tax number.

New technological dynamics

New dynamics brought about by technological advancements is a concern for governments looking to legislation to combat fake news. For example, Justice Ministers in three German states 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 US election.

Jenna Abrams, a popular Twitter account that garnered up to 70,000 followers through its support for US President Donald Trump and advocacy of far-right views, for example, is believed to have been run by the Russian propaganda machine to discredit the Democrats. The role of automated accounts in influencing elections was raised during the US Senate hearings as well.


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 US 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.”

Non-legislative measures

Legislation alone is insufficient in countering fake news and would expectedly be an on-going subject of study. Some countries prefer to beef up existing legislation instead of introducing new ones.

In Indonesia, online smear campaigns have affected electoral candidates’ standing in elections since 2012. There is 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 syndicate that creates many social media accounts to spread hate speech for clients willing to pay for them. Online sectarian narratives had polarised public opinion in the lead-up to the Jakarta gubernatorial elections in 2017 that saw the defeat of former governor, Basuki Tjahaja Purnama, a Chinese Christian. The Indonesian government hence has beefed up existing

legislation not only by introducing new provisions but also by issuing guidelines to aid their implementation and stepping up enforcement such as forming the Police Multimedia Bureau in 2017. This Bureau may be similar to the Centre Against Terrorism and Hybrid Threats in the Czech Republic, which also aims to counter disinformation campaigns.

Some countries prefer to implement non-legislative measures such as fact-checking and countering fake news websites. Malaysia has introduced an information verification website (Sebenarnya.my) to counter fake news while Qatar had launched the “Lift the Blockade” website to fight disinformation campaigns and provide its own perspective.

Non-legislative measures may also inculcate media literacy and critical thinking. Countries such as Canada, Italy, and Taiwan are introducing

---

29 In 2015, the Indonesian National Police issued Circular SE/06/X/2015 to guide law enforcement in implementing existing legislation against hate speech. See Azyumardi Azra, “Hate Speech and Freedom,” Republika, November 05, 2015, http://www.republika.co.id/berita/en/resonance/15/11/05/nxc601317-hate-speech-and-freedom. See also Abubakar, “Managing hate speech or muzzling freedom of expression?”
33 See Appendix B.
school curriculum that teaches children to discern between false and credible information. In recognising the role of online opinion leaders, some country leaders such as Indonesian President Joko Widodo has encouraged social media influencers to fight fake news by promoting unity.

Governments are also funding research on using technology such as artificial intelligence (AI) and machine learning (ML) to counter fake news. The US National Science Foundation has supported projects such as ClaimBuster, which uses natural language processing techniques to spot factual claims within texts. ClaimBuster has been used to check facts during the 2016 US presidential election. 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.

Recommendations

Due to the speed and wide reach of information dissemination, as well as the ambiguity of what exactly constitutes fake news, attempts to legislate fake news will inevitably face challenges.

Legal measures to target fake news may result in unexpected scenarios. First, removing fake news may give rise to the “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

36 See Appendix B.
officially sanctioned newspapers as government propaganda. In this state, netizens are more likely to seek and trust news from alternative sources than before. Second, 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.

Given the aforementioned challenges, a multi-pronged approach (see Fig. 1) 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 countering fake news.

**Pre-emptive measures**

To combat fake news, pre-emptive measures that are conducted in a collaborative manner should be taken. An issue-focused approach is formed for particular purposes such as elections. This allows targeted definition of fake news in a particular context, thus expediting the identification of related fictitious information. Collaboration on the other hand (i) facilitates the exchange of knowledge and skills; (ii) narrows the gap between local and global; (iii) helps identify overlapping concerns between different issues and contexts; and (iv) 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, 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.”42 The social media giant also terminated 30,000 accounts in France43 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.44 First Draft, a project of the Harvard Kennedy School’s Shorenstein Center that led fact-checking initiatives of Google-backed CrossCheck (France) and WahlCheck17 (Germany), is other example of pre-emptive collaborative actions that focused on a particular issue, namely elections.45

45 See section on Extra-Governmental Collaborations.
Collaborative engagements

Collaborations to combat fake news may comprise: (i) regional engagements; (ii) non-governmental collaborative efforts; and (iii) government-industry partnerships. The cooperating entities should agree on the rules of engagement, actions that have to be taken in a given timeline, and the responsibilities of each party. In the course of collaboration, rules of engagement have to be revised in light of changing conditions and adjusted according to the outcomes of implemented policies.

Regional collaborations: combating fake news in ASEAN

Fake news should be countered through concurrent efforts at the regional and international forums to share experiences and collaborate in mutually acceptable areas. For ASEAN Member States (AMS), the roundtable in September 2017 by the ASEAN Ministers Responsible for Information (AMRI) has set the stage for regional collaboration.46

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 says, but also its presentation, author, format, as well as context.47

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.48 The task force serves as a regional mechanism that enables collaboration with a

---


wide network of government officials, experts, journalists, and think tanks.\textsuperscript{49} The task force’s activities dovetail with the strategic communications activities of NATO, which include countering the use of disinformation campaigns by Russia for its geopolitical goals (e.g., in Ukraine).\textsuperscript{50}

While the EU and NATO’s models centre 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 2017 AMRI meeting, regional efforts to counter fake news could be subsumed under the actions plan of the ASEAN Socio-Cultural Community.

**Extra-governmental collaborations**

Extra-governmental alliances should form part of the framework for countering fake news. StopFake, for instance, is a multi-pronged initiative created by Kyiv Mohyla Journalism School and the KMA Digital Future of Journalism project in 2014 in Ukraine. It is supported by the efforts of IT professionals, translators, journalists, and others concerned about inaccurate information.\textsuperscript{51} Its main goal is to counter Russian disinformation operations and assess the impact of fake news in Ukraine and other countries.\textsuperscript{52} StopFake offers opinion pieces, insight to Russian disinformation operations, access to researches, guidance on verifying information, and videos debunking fake news, which are broadcasted on their site and local television.\textsuperscript{53}

First Draft is another initiative that brings together a “non-profit coalition” against disinformation. The coalition comprises: (i) technology companies (e.g., Google News Lab, Facebook, and Twitter); (ii) academic and research institutions (e.g., University of Southern California Annenberg School of Communication


\textsuperscript{52} Ibid.

and Journalism, Tufts Fletcher School, and Public Data Lab); (iii) newsrooms (e.g., The Washington Post, Reuters, and The Guardian); and (iv) other similar-minded organisations (e.g., FactCheck Initiative Japan and Now This). First Draft helped counter fake news during the French elections with its CrossCheck initiative, which congregated 37 newsrooms in France and UK to identify and debunk election-related fake news. During the German elections, First Draft, in cooperation with CORRECTIV, a “non-profit investigative newsroom” for German speakers, spearheaded a similar initiative called WahlCheck 17. Yet another initiative, the International Fact Checking Network, has been coordinating and training fact-checkers around the world.

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.

Government-industry partnerships

Striking the right balance between data security and countering fake news is an ongoing 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, could create a digital ambassador to engage with technology companies to determine how best to increase collaboration and minimise disputes.

Immediate measures

Immediate measures comprise transparent, timely, and accurate communication 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 relevant.

Other immediate measures include fake news flagging initiatives and fact-checking websites. Fake news flagging allows 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.

An environment of trust is necessary for immediate measures to be effective. Governments need to retain public trust through continuous, transparent communication with the public but this can be challenging especially during times of conflicting information. Non-governmental organisations (NGOs) comprising experts in the issues of interest can play a part due to their impartiality. For example, the Ukraine Crisis Media Center conducts “daily briefings,” “roundtables,” and “discussions” to unpack complex information on Ukraine and beyond.60

Long-term measures: media literacy and social norms

Long-term measures to counter fake news include: (i) initiatives to inculcate media literacy in schools that the elderly may also find useful;61 (ii) encouraging social norms62 against fake news such as responsible information sharing

61 The Italian government has collaborated 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.
62 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.
practices; and (iii) defining the responsibilities of technology companies in
countering fake news within the spectrum of collaborative engagements.

Legislating fake news: a silver bullet?

It is currently too early to assess the negative and positive impacts of
legislative initiatives against fake news. However, any attempt to legislate
against fake news would inevitably meet with difficulties given: (i) issues on
the definition of fake news; (ii) the global dimension of cyberspace vis-à-vis
the territorial boundaries of legislation; (iii) challenges in identifying the actual
perpetrator of fake news; and (iv) sophistication of disinformation campaigns.
Content-related regulations in cyberspace would also face obstacles.

First, it is important yet difficult to “reconcile” online regulations with offline
regime. For instance, while pornography is illegal in many Asian countries,
it is challenging to regulate such content in cyberspace. Second, variation
in terms of what is legal and illegal in different countries means that
“foreign undesirable materials” might 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. 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 despite Germany’s efforts to
restrict access to them.

Singapore has the necessary resources to adopt a comprehensive
approach that incorporates the abovementioned pre-emptive, immediate,
and long-term remedies to counter fake news. Moving forward, Singapore
could consider establishing an organisation – possibly non-governmental –
that uses grassroots participation to counter fake news. This organisation
could carry out research and fact-checking initiatives, congregate various

63 Responsible information sharing practices include crosschecking, authenticating the
source and the author as well as reading the information in full before sharing.
64 Hwa, “Framework,” 335.
65 Ibid.
66 Ibid.
67 Ibid, 338.
68 Ibid.
experts under it, and provide support for crisis communication specific to disinformation operations. Akin to the StopFake initiative in Ukraine, this institution could: (i) produce content for broadcast, print, and social media to inform the public; (ii) offer trainings to media professionals and other relevant parties; and (iii) educate digital information consumers through alternative means such as incorporating gamification into fake news identification.

This organisation could also collaborate with various government bodies to implement immediate and long-term solutions. These solutions may include expanding policies on media literacy and critical thinking; devising initiatives to establish healthy media consumption behaviours (e.g., information verification and reading the entire piece) as social norms; and assist in the implementation of the aforementioned measures. The benefit of establishing such an organisation is that it can help to win the trust of citizens given its impartial stance, and integrate citizens in the fight against fake news. An extra-governmental entity can thus serve as a bridge that facilitates public-private partnership, establishing trust that result in constructive actions benefitting the government, industry, and society as a whole.

Conclusion

Moves worldwide to enact legislation against fake news are generally at a nascent stage, with it being too early to attempt any holistic impact assessment. However, it is already clear that legislation must be contemplated only as one part of a multi-pronged strategy. Such a strategy should incorporate pre-emptive issue-focused measures, including collaborations with a wide variety of actors and organisations (e.g., regional organisations, NGOs, and technology companies), and it should encompass immediate responses such as crisis communication and fact-checking measures, and long-term remedies such as media literacy and fostering appropriate social norms.
# Appendix A

## Global Overview of Fake News Legislation (as at January 2018)

<table>
<thead>
<tr>
<th>Country</th>
<th>Legislation</th>
<th>Prescriptive actions</th>
<th>Accountable party</th>
<th>Tech company responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Germany</td>
<td>Approved</td>
<td>The Network Enforcement Act imposes fines on social media as much as 50 million euros (US$53 million) if they fail to remove “obviously illegal” content 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.</td>
<td>Technology companies</td>
<td>Facebook noted that 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.</td>
</tr>
<tr>
<td>Pending</td>
<td>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.</td>
<td>Unknown</td>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>


<table>
<thead>
<tr>
<th>Country</th>
<th>Legislation</th>
<th>Prescriptive actions</th>
<th>Accountable party</th>
<th>Tech company responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Italy</td>
<td>Pending</td>
<td>A legislative proposal, submitted on 7 February 2017 in the Senate of the Republic, provides for the adoption of Article 656-bis of the Criminal Code. Individuals who publish or circulate fake news, exaggerated, or biased information online that mislead shall face fines of up to EUR 5,000. This provision would apply only to online publications, which are not registered as “online newspapers”. The proposed legislation does not appear to address extraterritorial application.</td>
<td>Individuals</td>
<td>Nil</td>
</tr>
<tr>
<td></td>
<td></td>
<td>All 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 punishable with fines between €500 and €2,000.</td>
<td>Website administrators</td>
<td>Nil</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Internet Service Providers (ISPs) must monitor content, especially those that generate a substantial degree of interest among users, in order to assess the reliability and truthfulness of the content. If the ISP determines that certain content does not meet this requirement, it must promptly remove the content in question or face fines.</td>
<td>Internet Service Providers</td>
<td>Nil</td>
</tr>
<tr>
<td>Country</td>
<td>Legislation</td>
<td>Prescriptive actions</td>
<td>Accountable party</td>
<td>Tech company responses</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------------------------------</td>
<td>---------------------------------------------------------------------------------------</td>
<td>------------------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>The Philippines</td>
<td>Pending</td>
<td>The proposed Senate Bill No. 1492 entitled an “An Act Penalizing the Malicious Distribution of False News and Other Related Violations” 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.” Any person proven guilty of being involved in creating or distributing fake news will face fines and imprisonment. If the offender is a public official, he will have to pay twice the amount of fine and serve twice the period of imprisonment, disqualified from holding any public office. Mass media enterprise or social media platforms that fail, neglect, or refuse to remove false news will face fines and imprisonment. The proposed bill does not address extraterritorial application.</td>
<td>Individuals and technology companies</td>
<td>Nil</td>
</tr>
<tr>
<td>Country</td>
<td>Legislation</td>
<td>Status</td>
<td>Prescriptive actions</td>
<td>Accountable party</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>--------</td>
<td>----------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Russia</td>
<td>Pending</td>
<td>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. The law would apply to individuals and large corporations. The proposed bill does not appear to address extraterritorial application.</td>
<td>One of the law’s authors, Deputy Sergey Boyarsky, assured 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.”</td>
<td>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.</td>
</tr>
<tr>
<td>USA</td>
<td>Pending</td>
<td>The Honest Ads Act, a bipartisan bill, would require internet companies to disclose details on political advertisements placed on the companies’ platforms. The proposed Act will address extraterritorial application through seeking to prevent “contributions, expenditures, and disbursements for electioneering communications by foreign nationals in the form of online advertising.”</td>
<td>Technology companies</td>
<td>At 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 counter fake news.</td>
</tr>
<tr>
<td>Country</td>
<td>Legislation</td>
<td>Status</td>
<td>Prescriptive actions</td>
<td>Accountable party</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td>--------</td>
<td>----------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>UK</td>
<td></td>
<td>Pending</td>
<td>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. It is currently unclear if the Inquiry will look into legislation.</td>
<td>Technology companies</td>
</tr>
<tr>
<td>Australia</td>
<td>In progress</td>
<td>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.</td>
<td>Technology companies, online advertisers, and other parties who benefit from disinformation.</td>
<td>At the public hearing on 22 August 2017, Google and Facebook made a submission that includes actions undertaken to address fake news.</td>
</tr>
<tr>
<td>Israel</td>
<td></td>
<td>Pending</td>
<td>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.</td>
<td>Technology companies</td>
</tr>
<tr>
<td>Country</td>
<td>Legislation Status</td>
<td>Prescriptive actions</td>
<td>Accountable party</td>
<td>Tech company responses</td>
</tr>
<tr>
<td>---------</td>
<td>-------------------</td>
<td>----------------------</td>
<td>-------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>India</td>
<td>Approved</td>
<td>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 is found to be circulating on his/her social media group. The joint order does not address extraterritorial application.</td>
<td>Administrators of social media groups</td>
<td>Nil</td>
</tr>
<tr>
<td>Canada</td>
<td>Implemented</td>
<td>In October 2017, the Canadian Radio-Television and Telecommunications Commissions 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.</td>
<td>Mass media</td>
<td>Nil</td>
</tr>
</tbody>
</table>
## Government-Initiated Measures against Fake News (as at January 2018)

<table>
<thead>
<tr>
<th>Country</th>
<th>Status</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Qatar</td>
<td>Implemented</td>
<td>The Qatari government has launched a new website called “Lift the Blockade” to counter “fake news” amid the on-going Gulf crisis.</td>
</tr>
<tr>
<td>Malaysia</td>
<td>Pending</td>
<td>The Malaysian government has proposed making online websites (with high volumes of web traffic) register with the Malaysian Communications and Multimedia Commission (MCMC).</td>
</tr>
<tr>
<td></td>
<td>Implemented</td>
<td>The MCMC has set up a website (Sebenarnya.com 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.</td>
</tr>
<tr>
<td>Czech Republic</td>
<td>Implemented</td>
<td>In Jan 2017, the Ministry of Interior created a specialist unit named Centre Against Terrorism and Hybrid Threats to counter disinformation that threatens 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.</td>
</tr>
<tr>
<td>Indonesia</td>
<td>Implemented</td>
<td>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.</td>
</tr>
<tr>
<td>Taiwan</td>
<td>In progress</td>
<td>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 mechanisms. The Taiwanese government is also using vTaiwan, an online tool to involve citizens in exchanging views on how to fight against disinformation.</td>
</tr>
<tr>
<td>Country</td>
<td>Status</td>
<td>Actions</td>
</tr>
<tr>
<td>---------</td>
<td>----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Italy</td>
<td>In progress</td>
<td>The Italian government is collaborating with Facebook and Google to teach students across 8,000 high schools to recognise fake information.</td>
</tr>
<tr>
<td>Sweden</td>
<td>In progress</td>
<td>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 curriculum will also teach students how to discern reliable and unreliable sources.</td>
</tr>
<tr>
<td>Finland</td>
<td>Implemented</td>
<td>The Finnish government has hired US consultants to train Finnish officials to recognise and respond to fake news. Students are also taught to read news critically in schools.</td>
</tr>
<tr>
<td>China</td>
<td>Implemented</td>
<td>The Chinese military launched a website in November 2017 for the public to report leaks, fake news, and illegal online activities by military personnel.</td>
</tr>
<tr>
<td>Canada</td>
<td>Implemented</td>
<td>NewsWise is an initiative to equip Canadian students aged nine to 19 in news literacy.</td>
</tr>
<tr>
<td>USA</td>
<td>Implemented</td>
<td>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 US 2016 presidential election and 2017 Australian Parliament discussion on topics of national interest such as budget and citizenship.</td>
</tr>
</tbody>
</table>
About the Authors

**Gulizar Haciyakupoglu** is a Research Fellow at the Centre of Excellence for National Security (CENS), S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU). Her research interests include disinformation campaigns in cyberspace; online trust; the interplay between Internet, communication and authority; gender equality advocacy in cyberspace; and feminism in Islam. She holds a Ph.D. from the National University of Singapore (NUS), Communications and New Media Department (CNM), and a MA on Political Communication from the University of Sheffield. She received her bachelor’s degree on Global and International Affairs from the Dual-Diploma Program of the State University of New York (SUNY) Binghamton and Bogazici University Turkey. Before embarking on an academic career, she worked as a Channel Sales Manager at IBM Turkey.

**Jennifer Yang Hui** is an Associate Research Fellow at the Centre of Excellence for National Security (CENS), a constituent unit of the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU). Jennifer has an Honours degree in History from the National University of Singapore (NUS). In 2010, she graduated as a Tun Dato Sir Cheng Lock Tan Master of Arts (M.A.) scholar in Southeast Asian Studies, also from NUS. Prior to joining CENS, Jennifer had worked at the National Archives of Singapore and the Institute of South East Asian Studies (ISEAS). While in CENS, Jennifer is responsible for research in Social Media Analytics. Her other research interests are security sector reform, ethno-religious relations, and the role of the social media in contemporary Indonesia, epistemology, knowledge making and their implications on digital maturity.

**V. S. Suguna** is an Associate Research Fellow with the Centre of Excellence for National Security (CENS) at the S. Rajaratnam School of International Studies (RSIS). She holds a Master of Strategic Studies from RSIS with a Certificate in Terrorism Studies and a Bachelor of Computing (Computer Engineering) from the National University of Singapore. Prior to joining RSIS, Suguna has served as a Staff Officer (Technology Branch) with the Singapore Prison Service (SPS) and was a Senior Executive in the Crisis Preparedness Directorate of the Joint Operations Group (JOG) at the Singapore Ministry of Home Affairs (MHA) where she helped coordinate
inter-agency crisis exercises and facilitated international engagements for sharing of best practices in crisis management. She is also a recipient of the Commissioner of Prisons Team award in 2015 recognising her efforts in the implementation of the Electronic Letters and other projects for SPS. Her research interests are in understanding the psychological drivers of cybercrime and studying the dynamics of social resilience.

Dymphles Leong is a Senior Analyst with Centre of Excellence for National Security (CENS) at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University, Singapore. She attained her Bachelor of Business majoring in Marketing and Management from the University of Newcastle Australia. Her research interests revolve around strategic communications, social media, communication, and global studies. She currently researches in the areas of behavioural insights and policymaking, digital activism, and civic engagement online. Her commentaries have been published in newspapers such as The Straits Times and the New Straits Times.

Muhammad Faizal is a Research Fellow with the Centre of Excellence for National Security (CENS), at the S. Rajaratnam School of International Studies (RSIS). He holds a Bachelor of Business Administration (with Merit), from the National University of Singapore. Prior to joining RSIS, Faizal served with the Singapore Ministry of Home Affairs where he was a deputy director and had facilitated international engagements with foreign security counterparts. He also had postings in the Singapore Police Force where he supervised and performed intelligence analysis, achieving several commendation awards including the Minister for Home Affairs National Day Award (2009), for operational and analysis efficiency; and in the National Security Research Centre (NSRC), at the National Security Coordination Secretariat (NSCS), where he led a team to research emergent trends in domestic security and monitor terrorism-related developments. Faizal also has certifications in Counter-Terrorism, Crime Prevention, and Business Continuity Planning.
About the Centre of Excellence for National Security

The Centre of Excellence for National Security (CENS) is a research unit of the S. Rajaratnam School of International Studies (RSIS) at the Nanyang Technological University, Singapore.

Established on 1 April 2006, CENS’ raison d’être is to raise the intellectual capital invested in strategising national security. To do so, CENS is devoted to rigorous policy-relevant analysis across a range of national security issues.

CENS is multinational in composition, comprising both Singaporeans and foreign analysts who are specialists in various aspects of national and homeland security affairs. Besides full-time analysts, CENS further boosts its research capacity and keeps abreast of cutting-edge global trends in national security research by maintaining and encouraging a steady stream of Visiting Fellows.

For more information, please visit www.rsis.edu.sg/research/cens/.

About the S. Rajaratnam School of International Studies

The S. Rajaratnam School of International Studies (RSIS) is a professional graduate school of international affairs at the Nanyang Technological University, Singapore. RSIS’ mission is to develop a community of scholars and policy analysts at the forefront of security studies and international affairs. Its core functions are research, graduate education, and networking. It produces cutting-edge research on Asia Pacific Security, Multilateralism and Regionalism, Conflict Studies, Non-traditional Security, International Political Economy, and Country and Region Studies. RSIS’ activities are aimed at assisting policymakers to develop comprehensive approaches to strategic thinking on issues related to security and stability in the Asia Pacific.

For more information, please visit www.rsis.edu.sg.