LAKSHMAN KADIRGAMAR INSTITUTE
OF INTERNATIONAL RELATIONS AND STRATEGIC STUDIES

POLICY BRIEFS

Policy Briefs Series: No.20

LKI *Policy Briefs* are extended analyses on foreign policy issues.

Tech Giants, *'TechPlomacy'* and Mitigating Online Radicalization: Lessons for Sri Lanka

Sandunika Hasangani *

January 2020

***Sandunika Hasangani** is a Research Fellow at the Lakshman Kadirgamar Institute of International Relations and Strategic Studies (LKI). The opinions expressed in this piece are the author's own and not the institutional views of LKI, and do not necessarily reflect the position of any other institution or individual with which the author is affiliated.

About LKI *Policy Briefs*

LKI Policy Briefs are extended analyses on foreign policy issues.

Terms of use

Lakshman Kadirgamar Institute of International Relations and Strategic Studies
24 Horton Place, Colombo 7, Sri Lanka
Email: programmes@lki.lki. Website: www.lki.lk

Contents

In today's interconnected world, technological advances, digitization, and online human behavior indubitably play a dominant role in foreign and national security policies of states. This was clear during the last few years of sporadic social media instigated ethno-religious riots across Sri Lanka, that culminated with the post-Easter Sunday ethnic tensions in April 2019. Christchurch attack and the way it was live-streamed on social media is another side of the same story. There is an increased attention on to what extent internet consumption feeds radicalization/spread of violence, and how to mitigate that. While tech companies should self-govern content on their own platforms, states undeniably also need to play an active role. The key question is how small countries like Sri Lanka should moderate its citizen's behavior online, leverage the giant tech companies, and manage the digital statecraft right? This LKI *Policy Brief* suggest that Sri Lanka considers a three-tier 'TechPlomacy' policy that includes (1) Silicon Valley diplomacy, (2) national digital/cyber security policies and (3) regionalism, in order to standardize the state's involvement in national security issues emerging from the world of Internet of Things (IoT).

> *"Diplomacy has shifted. We aren't in the 1900s anymore; we're not in a world where it's all about bilateral relations with other countries. Countries need to adapt their view of diplomacy to counter that. The [tech] companies will have significant influence on the world, and you can either step back and watch that happen or you can work with that."*
>
> - Priya Guha (Britain's former Consul General in San Francisco)

I. Introduction

By the end of 2019, 4.1 billion people used the internet,[1] with nearly a third of the world's population active on Facebook alone.[2] Estimates project that the internet and social media usage continues to rise in developing and emerging economies.[3] In Sri Lanka, approximately 6.73 million people are using the internet and there are 6.2 million active social media users accounting for 30% of the entire population.[4]

As many people have moved online, witnessing textual and visual contents of hate speech, xenophobia, and racism is a frequent reality on social media platforms. Facebook removed more

than seven million instances of hate speech in the third quarter of 2019.[5] We also witnessed how social media instigated violence during the last decade. For instance, in March of 2018, the Government of Sri Lanka (GoSL) temporarily blocked public access to social media for the first time in its history after communal violence erupted in Kandy. This turning point was blamed on the risk of interfaith and inter-ethnic disharmony stimulated by social media.[6] Most recently, after the Easter Sunday bombings in April 2019, allegedly several ethnic disturbances were triggered by certain posts on social media, indicating the importance of further research on the way human behavior on virtual spaces creates real-life impact. According to the data produced by the Sri Lanka Computer Emergency Response Team (CERT), among all the reported cyber security related incidents, social media incidents are the most prevalent with exponential increase noted from 80 incidents in 2010 to 3685 in 2017.[7]

Given this context, there is an increased necessity to govern online human behaviors at different levels. While tech giants have a greater responsibility to self-govern the contents on their own platforms, actions should also be taken at the national level. The key question is *how small states like Sri Lanka should moderate its citizens' behavior online, leverage the giant tech companies and manage their digital statecraft right?* Below, the author first briefly discusses what *TechPlomacy* and online radicalization means, and some of the self-governing measures taken by tech giants. Secondly, the paper focuses on the national level, and suggests three key policy areas that should be integrated in a national *TechPlomacy* policy. First, Sri Lanka should focus on constructing a proper line of communication with tech giants which is rephrased here as 'Silicon Valley Diplomacy.' Secondly, Sri Lanka needs to carefully craft national policies (digital and cyber security policies) to govern online well-being of her citizens. Thirdly, smaller states should seek possible avenues to benefit from regionalism to mitigate online radicalization and spread of violence.

II. Defining *TechPlomacy* and Online Radicalization

2.1 ***TechPlomacy***: Its Scope and Validity

TechPlomacy, or technological-diplomacy, is one of the newest additions to the field of diplomacy. This includes state initiatives to create constructive dialogues with the giant tech companies (such as Facebook, Amazon, or Alibaba) to minimize national security and economic issues emerging

through the advances of technology. The concept is based on the primary assumption that technical advances could create security threats to modern nation-states.

Denmark was the first country to adopt a *TechPlomacy* policy in mid-2017, considering technical advances, digitization, and human behaviors online as a cross-cutting national security and foreign policy priority. This initiative aims at addressing three interlinked trends in foreign policy today: (1) the fourth industrial revolution is responsible for today's most far-reaching societal changes such as social media and elections, protection of personal information and human rights (2) the power of giant tech companies (arguably) surpasses the power of traditional nation states, and policy makers at all levels are struggling to keep up with the pace and impact of tech companies (3) emerging technological advances are increasingly shaping the foreign policies and geopolitics in new ways. For instance, 5G networks have become a controversial issue internationally.[8] Danish *TechPlomacy* is operationalized by its tech ambassador who has a global mandate, and a physical presence across three-time zones: Silicon Valley, Copenhagen, and Beijing. The tech embassy brings forward concerns and questions on behalf of Danish authorities with tech companies and influences the international agenda around tech policy considerations.[9]

While *TechPlomacy* in the Danish usage primarily means the establishment of the tech embassy and its global mandate (spanning international communications and activities), *TechPlomacy* in this paper is given an encompassing scope to cover a range of activities from national policy formation to technological-diplomacy practiced outside the national boundaries. Against this broader view, this policy brief identifies three tiers of policy reforms that Sri Lanka needs to consider carefully in order to meet her rising internet-based national security issues (such as online radicalization).

2.2 Online Radicalization: Algorithms vs. Psychological Biases

Radicalization means the adoption of beliefs and attitudes that are in opposition to the mainstream status quo and dominant socio-political discourse.[10] However, scholars also argue that the adoption of radical views and beliefs are not necessarily negative or dangerous[11] for the greater public. Therefore, alternatively, scholars suggest that radicalization becomes a social concern only when it leads to beliefs and attitudes that sanction, legitimize and compel violence as a means to achieve social change.[12] Especially, when radical views and beliefs develops into "a willingness to directly

support or engage in violent acts,"[13] such scenarios are called violent radicalism and need to be prevented, monitored or de-radicalized.

Online radicalization is essentially related to the IoT[14] and there is a dichotomous explanation of the sources behind online radicalization. First, do technological advances (i.e. proprietary algorithms) increase the tendency of online radicalization? And second, does it depend on the psychological biases of the user? These two questions should be carefully answered by future researchers and such data should be fed into the policy making processes.

When reviewing prevailing literature, those who advocate the effect of algorithmic curation over between-person differences of information consumption identify 'filter bubbles' and 'echo chambers' as the source of the problem. Their rationale is based on algorithms, which are intended to personalize the user's online experience based on the data provided by the user himself placing the user in a bubble. Thus, the user consumes content similar to what he consumed before, and consequently is not exposed to contents beyond his choice. Recent studies have identified the presence of ideological and partisan echo chambers in Twitter discussions,[15] and in Facebook groups and pages.[16] Another study conducted in 2017 concludes that customizable technology increased ideologically-driven selective exposure and the likelihood of filter bubbles in the modern media landscape.[17]

The second possible source behind social media instigated online radicalization is the user's psychological biases. Four major concepts cover the psychological biases of media consumers. 'Selective exposure,' meaning individuals tend to consume media which aligns with their views and beliefs, 'confirmation bias,' which refers to the human tendency to seek evidence to support the hypothesis in hand, 'availability bias,' meaning that information that can be most easily retrieved from human memory tend to dominate the decision-making process, judgements and opinions, and finally the 'news-find-me perception,' which refers to human inactivity in actively seeking out information due to the high-choice media environment.

Currently, Sri Lanka lacks specific data on the relative importance of algorithms and the psychological biases of social media users in radicalization. Such knowledge and data will be highly effective in future policy making attempts, specifically in designing preventive measures. Globally, previous research finds that radicalization online/on social media is more driven by

psychological biases (i.e. selective exposure), rather than algorithms (filter bubbles or echo chambers).[18] Yet, there could be context specific differences which we still need to explore.

III. Tech-Giants and Self-Governance of Online Content

Tech-giants like Facebook, Twitter, and YouTube are increasingly researching on innovative methods of governing millions of contents published on their platforms daily. This online content appears in two major primary forms: textual and visual. The latter includes variety of sub-forms such as images, videos, and memes. Below, some of the recent efforts to prevent the dissemination of hate speech, misinformation in both textual and visual contents have been briefly listed while identifying some gaps that still require attention.

3.1 Efforts of Governing Textual Contents

In 2018, Facebook introduced two updates to its newsfeed: first to assure that people consume fewer public contents, including news, videos, and posts from brands on their newsfeed. Second to assure that people consume high quality news from trustworthy, informative, and local sources. According to Zuckerberg, this is a measure introduced to tackle sensationalism, misinformation, and polarization on social media. Trustworthiness is judged as a part of Facebook's ongoing quality surveys, where Facebook "ask people whether they're familiar with a news source and, if so, whether they trust that source. The idea is that some news organizations are only trusted by their readers or watchers, and others are broadly trusted across society even by those who don't follow them directly."[19] This will change the balance users consume towards sources that are determined to be trusted by the community. Facebook is prioritizing trusted sources in India, UK, Germany, France, Italy, Spain, and Brazil.

3.2 Managing Visual Contents

For videos and photos, Facebook has introduced "visual verification techniques, such as reverse image searching and analyzing image metadata such as when and where the photo or video was taken. Fact-checkers are able to assess the truth or falsity of a photo or video by combining these skills with other journalistic practices, making use of research from experts, academics, or

government agencies."[20] Facebook is also using optical character recognition (OCR) to extract text from photos and compare that text to headlines from fact-checkers' articles.[21]

A large amount of data consists of images with text. For instance, it could be a meme with text overlay or photo of a billboard. In order to govern such photos that contain overlaid text, Facebook has built and deployed a large-scale machine learning system named Rosetta. It extracts text from more than a billion public Facebook and Instagram images and video frames (in a wide variety of languages), daily and in real time, and inputs the information into a text recognition model that has been trained on classifiers to understand the context of the text and the image together.[22]

IV. Policy Recommendation I: Silicon Valley Diplomacy

Silicon Valley diplomacy is still a new concept for Sri Lankans and for the rest of the developing world. The basis of this concept is that states are no longer the key actors of global power politics, but giant tech companies are increasingly accumulating global power and control of international affairs. Therefore, states need to reconsider their foreign policies depending on the newest technological advances, as well as updating the diplomatic tools by training and posting career diplomats to represent national interest before tech companies. As the world's first career Tech diplomat, Casper Klynge who represents Denmark's interests before companies such as Facebook and Google, articulates, "our values, our institutions, democracy, human rights, in my view, are being challenged right now because of the emergence of new technologies. These companies have moved from being companies with commercial interests to actually becoming de facto foreign policy actors."[23]

For vulnerable societies like Sri Lanka, where modern ethnic tensions are instigated through human behaviors online, Silicon Valley diplomacy is an essential tool to be practiced. However, Sri Lanka being a relatively smaller market with 6.73 million internet users and 6.2 million active social media users, it is unlikely that giant tech companies like Facebook, Google, or YouTube will voluntarily address the context specific internal issues arising from internet/or social media consumption. Therefore, Sri Lanka needs to establish a proper channel of communication with Silicon Valley.

4.1 Silicon Valley Diplomacy and Eliminating Online Radicalization in Sri Lanka

Sri Lanka needs to craft a proactive strategy to engage with the tech giants in Silicon Valley. Repercussions of the absence of such a policy were well visible in the aftermath of both Digana Buddhist-Muslim riots in March 2018, and post-Easter Attacks in April 2019. Both cases provide examples of reactive measures taken by both Facebook and the GoSL, which banned access to social media temporarily as it was understandably the fastest way to reduce dissemination of hate speech. Both the government and some civil society organizations in Sri Lanka were critical of Facebook for not hiring content reviewers for Sri Lanka, and the absence of Artificial Intelligence (AI) and other technological capacities to control the spread of ethnic rage on Facebook.[24]

Although the reactive measures taken by both parties were useful, Sri Lanka needs to invest in a proactive approach to Silicon Valley diplomacy. Appointing a Sri Lankan tech ambassador could be useful, but prior to that it is essential to study the success cases (such as Danish *TechPlomacy*) and priorities in Sri Lanka. Possibly a range of issues will fall under the mandate of Sri Lankan *TechPlomats* such as online misinformation and hate speech, content moderation, data privacy, human rights, cyber security, and taxation. Each of these specific fields (and possible other areas) should be integrated in the national *TechPlomacy* policy and the relevant officials should be educated and trained in representing Sri Lanka in the Silicon Valley.

V. Policy Recommendation II: Developing National Policies

There is a published Cyber Security Strategy for Sri Lanka developed by the Sri Lanka CERT,[25] and a draft National Digital Policy for 2020-2025 drafted by the Ministry of Digital Infrastructure and Information Technology (MDIIT). Overall, Sri Lanka has set some progressive steps to meet the phase and scope of issues emerging from digitization and technological advances. However, in addition to the above, below the author focuses on several key policy areas that need further attention.

5.1 Local Laws to Regulate Violent Content Online

Filling the existing legal gap, the Ministry of Defense is to introduce new laws to stop defamatory posts and comments on social media and also set up a mechanism for immediate removal of

ethically and religiously sensitive posts that spread hatred via social media networks. This new legal framework will be introduced under the National Cyber Security Strategy, and the Digital Infrastructure Protection Agency (DIPA) will be newly set up as an apex body for all cyber security related affairs. [26]

There are a few internationally adopted laws that can also set examples for local policymakers/lawmakers in Sri Lanka. For instance, in Germany, NetzDG law came into effect at the beginning of 2018, applying to companies with more than two million registered users in the country. These companies were forced to set up procedures to review complaints about content they are hosting and remove anything that is clearly illegal within 24 hours. Individuals may be fined up to €5m ($5.6m; £4.4m) and companies up to €50m for failing to comply with these requirements.[27]

Similarly, Australia passed 'Sharing of Abhorrent Violent Material Act' in the aftermath of the Christchurch attack, introducing criminal penalties for social media companies, possible jail sentences for tech executives for up to three years and financial penalties worth up to 10% of a company's global turnover.[28] Although it is clear that lawmaking is controversial in this field, given the magnitude of damage (for social harmony) caused during the last few years, it is high time that the GoSL focuses on proper laws that regulate hate speech and misinformation online.

5.2 Developing an Index of Radical Tropes and Slur in Local Languages

There is an increased demand for developing a public index of textual contents including radical/violent slangs, idioms, tropes, and slur of all local languages. In the case of Sri Lanka this applies to Sinhala, Tamil as well as local usage of English slur and tropes as well. While strictly assigning responsibilities to a section of the society is essentially a narrower approach, the state agencies have more resources and expertise in pooling language corpuses compared to other non-state actors. For instance, Sri Lankan public universities along with the Department of Official Languages and the Ministry of National Integration and Reconciliation can be coordinated for such a task. That said, developing such a corpus is useless unless data is prepared in a format that can

be fed into a machine-learning system which requires the coordination and collaboration between language specialists and ICT specialists.

5.3 Counter-Narrations on Social Media

Developing counter-narratives by states has been another popular (yet controversial) approach of preventing online radicalization. Counter-narratives are strategically constructed storylines that are projected and nurtured through strategic communication (or messaging) activities with the intention to undermine the appeal of extremist narratives of violent extremist groups. Several methods of counter-narratives exist, such as: (1) counter messaging (e.g. activities that challenge extremist narratives); (2) alternative messaging (e.g. activities that aim to provide a positive alternative to extremist narratives); and (3) strategic communication by the government (e.g. activities that provide insight into what the government is doing).[29] However, developing counter-narrative includes several cautions. First, who should develop and disseminate counternarratives? Second, if the responsibility lies with state agencies, is there a possibility of ensuring the political and ideological correctness of state narrations? These concerns are sensitive areas that should be tackled carefully when adopting counter-narratives as a preventive measure of online radicalization.

VI. Policy Recommendation III: Regionalism and Its Benefits

While states can communicate with tech companies directly as discussed in the previous section, regional initiatives are also proven effective. Specifically, Sri Lanka being a smaller market for many of the leading technological companies, and also being a smaller state in terms of political and economic influence, Silicon Valley diplomacy will be not only be challenging initially, but also be time consuming. Regionalism will be an effective substitution in this context.

The European Union (EU) is one of the success stories. In May 2016, the Commission agreed with Facebook, Microsoft, Twitter, and YouTube a 'Code of Conduct' on countering illegal hate speech online. The aim of the Code is to make sure that requests to remove content are dealt quickly. When companies receive a request to remove content deemed to be illegal from their online platform, they assess this request against their rules and community guidelines and, where necessary, national laws transposing EU law on combating racism and xenophobia. The companies

have committed to reviewing the majority of these requests in less than 24 hours and to removing the content if necessary, while respecting the fundamental principle of freedom of speech. As at the end of 2019, nine IT companies, including Instagram, Google+, Snapchat, Dailymotion, and jeuxvideo.com adhere to the Code of conduct. According to the 4th evaluation of the EU Code of conduct in 2018, IT companies are on average removing 72 percent of the illegal hate speech notified to them. In 89 percent of the cases IT companies assessed the notifications in less than 24 hours, meeting some of the public commitments agreed upon the Code of conduct.

Regional cooperation for governing hate speech and preventing online radicalization in the South Asian context is still at the initialization stage. For instance, the South Asian Association for Regional Cooperation (SAARC) has established a Cyber Crime Monitoring Desk in 2013, and The Bay of Bengal Initiative for Multi-Sectoral Technical and Economic Cooperation (BIMSTEC) has also initiated several policy-level dialogues on social media and radicalization.[30] South Asia and the Bay of Bengal region shows similarities of radicalization with shared history, religious and ethnic backgrounds, thus need to invest more on proactive measures to tackle online radicalization.

VII. Conclusion

While rapid technological advances, digitization, and the immense consumption of social media are essentially positive developments, they have simultaneously endangered the national security and altered the foreign policy priorities of states. For instance, the rapid spread of radicalization across geographical, social, and gender boundaries is due to the wider presence of online tools. Giant tech companies move forward rapidly creating immense security issues, but states lag behind in addressing those. Smaller states like Sri Lanka need to watch the tech-developments and as this policy brief suggests a carefully crafted *TechPlomacy* is at high demand. As identified in the paper, Silicon Valley diplomacy, regionalism, and developing national policies are the priorities. Raising awareness among the general public is also imperative. Smaller states need to adopt creative methods to counter powerful tech giants and the goal should be to make sure that "democratic governments set the boundaries for the tech industry and not the other way around."[31]

Notes

[1]ITU. (2019). *Individuals Using the Internet, 2015-2019*. International Telecommunication Agency. [Online] Available at: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx [Accessed 20 January 2020].

[2]Laub, Z. (2019). *Hate speech on Social Media: Global Comparisons*. Council on Foreign Relations. [Online] Available at: https://www.cfr.org/backgrounder/hate-speech-social-media-global-comparisons [Accessed 20 January 2020].

[3]Jacob, P., Bishop, C. & Chwe, H. (2018). *Social Media use Continues to Rise in Developing Countries but Plateaus Across Developed Ones*. Pew Research Center. [Online] Available at: https://www.pewresearch.org/global/2018/06/19/social-media-use-continues-to-rise-in-developing-countries-but-plateaus-across-developed-ones/ [Accessed 20 January 2020].

[4] Datareportal. (2019). *Digital 2019 Sri Lanka*. [Online] Available at: https://www.slideshare.net/DataReportal/digital-2019-sri-lanka-january-2019-v01 [Accessed 20 January 2020].

[5]Perrigo, B. (2019). *Facebook says it's removing more hate speech than ever before. But there's a catch.* TIME. [Online] Available at: https://time.com/5739688/facebook-hate-speech-languages/ [Accessed 20 January 2020].

[6] Rasheed, Z. & Perera, A. (2018). *Did Sri Lanka's Facebook Ban Help Quell Anti-Muslim Violence?* [Online] Aljazeera. Available at: https://www.aljazeera.com/news/2018/03/sri-lanka-facebook-ban-quell-anti-muslim-violence-180314010521978.html [Accessed 20 January 2020].

[7]Sri Lanka CERT. (2018). *National Information and Cyber Security Strategy of Sri Lanka (2019-2023)*. Sri Lanka CERT. [Online] Available at: https://www.cert.gov.lk/index.php [Accessed 20 January 2020].

[8]Office of Denmark's Tech Ambassador. (2017 sic). *TechPlomacy*. [Online] Available at: https://techamb.um.dk/en/techplomacy/abouttechplomacy/ [Accessed 4 January 2020].

[9] Ibid.

[10]Macnair, L., & Frank, R. (2017). Voices Against Extremism: A case study of a community-based CVE counter-narrative campaign. *Journal for Deradicalization. 10*:147-174.

[11]Davies, G. et al. (2016). Toward a framework understanding of online programs for countering violent extremism. *Journal for Deradicalization. 6*: 51-86.

[12]Ibid.

[13]Dalgaard-Nielsen, A. (2013). Promoting exit from violent extremism: Themes and approaches. *Studies in Conflict & Terrorism. 36*(2):99-115.

[14]A system of interconnected devices each connected to the internet. These interconnected devices could include everything from smartphones, personal computers, to smart watches, lamps or a coffee machine.

[15]Barbera, P., Jost, TT., Naglar J. et al. (2015). Tweeting from left to right: Is online political communication is more than an echo chamber? *Psychological Science*. *26*(10):1531-1542.

[16]Jacobson, S., Myung, E., Johnson, SL. (2016). Open media or eco chamber: The use of links in audience discussions. *Information, Communication and Society*. *19*(7): 875-891.

[17]Dylko, I., et al. (2017). The dark side of technology: an experimental investigation of the influence of customizability technology on online political selective exposure. *Computer in Human Behavior 73*: 181-190.

[18]Spohr, D. (2017). Fake news and the Ideological Polarization: Filter Bubbles and selective Exposure on Social Media. *Business Information Review*. *34*(3): 157.

[19]Mosseri, A. (2018). *Helping ensure news on Facebook is from trusted sources.* [Online] Available at: https://newsroom.fb.com/news/2018/01/trusted-sources/
[Accessed 20 January 2020].

[20]Woodford, A. (2018). *Expanding fact-checking to photos and videos*. [Online] Available at: https://about.fb.com/news/2018/09/expanding-fact-checking/ [Accessed 20 January 2020].

[21] Ibid.

[22] Sivakumar, V., Gordo, A. & Paluri M. (2018). *Rosetta: Understanding text in images and videos with machine learning*. [Online] Available at: https://engineering.fb.com/ai-research/rosetta-understanding-text-in-images-and-videos-with-machine-learning/
[Accessed 20 January 2020].

[23]Satariano, A. (2019). *The World's First Ambassodar to the Tech Industry*. [Online] The New York Times. Available at: https://www.nytimes.com/2019/09/03/technology/denmark-tech-ambassador.html [Accessed 8 January 2020].

[24] Groundviews. (2018). *Open Letter to Facebook: Implement Your Own Community Standards.* Groundviews. [Online] Available at: https://groundviews.org/2018/04/10/open-letter-to- facebook-implement-your-own-community-standards/ [Accessed 8 January 2020].

[25] CERT Sri Lanka. (2018). *National Information and Cyber Security Strategy of Sri Lanka 2019-2023.* CERT Sri Lanka/Ministry of Digital Infrastructure and Information Technology. [Online] Available at: https://www.cert.gov.lk/Downloads/NCSStrategy.pdf [Accessed 20 January 2020].

[26]Daily FT. (2020). *Government to bring new laws to combat online hate speech*. [Online] Available at: http://www.ft.lk/front-page/Govt-to-bring-new-laws-to-combat-online-hate-speech/44-694230 [Accessed 24 January 2020].

[27]Eerten, J. et al. (2017). *Developing a social media response to radicalization: The role of counter-narratives in prevention of radicalization and de-radicalization*. Research and Documentation Center, Ministry of Security and Justice, Netherlands. [Online] Available at: https://dare.uva.nl/search?identifier=4fe0b95f-b5ec-45a1-b50a-2ff8287b4b1c. [Accessed 20 January 2020].

[28]Reality Check Team-BBC. (2019). *Social Media: How Can Governments Regulate it?* [Online] BBC. Available at: https://www.bbc.com/news/technology-47135058 [Accessed 20 January 2020].

[29] Ibid.

[30] BIMSTEC Secretariat. (2019). *Second BIMSTEC Think Tanks Dialogue on Regional Security*. BIMSTEC. [Online] Available at: https://bimstec.org/?event=second-bimstec-think-tanks-dialogue-on-regional-security [Accessed 13 January 2020].

[31] Supra note 22.