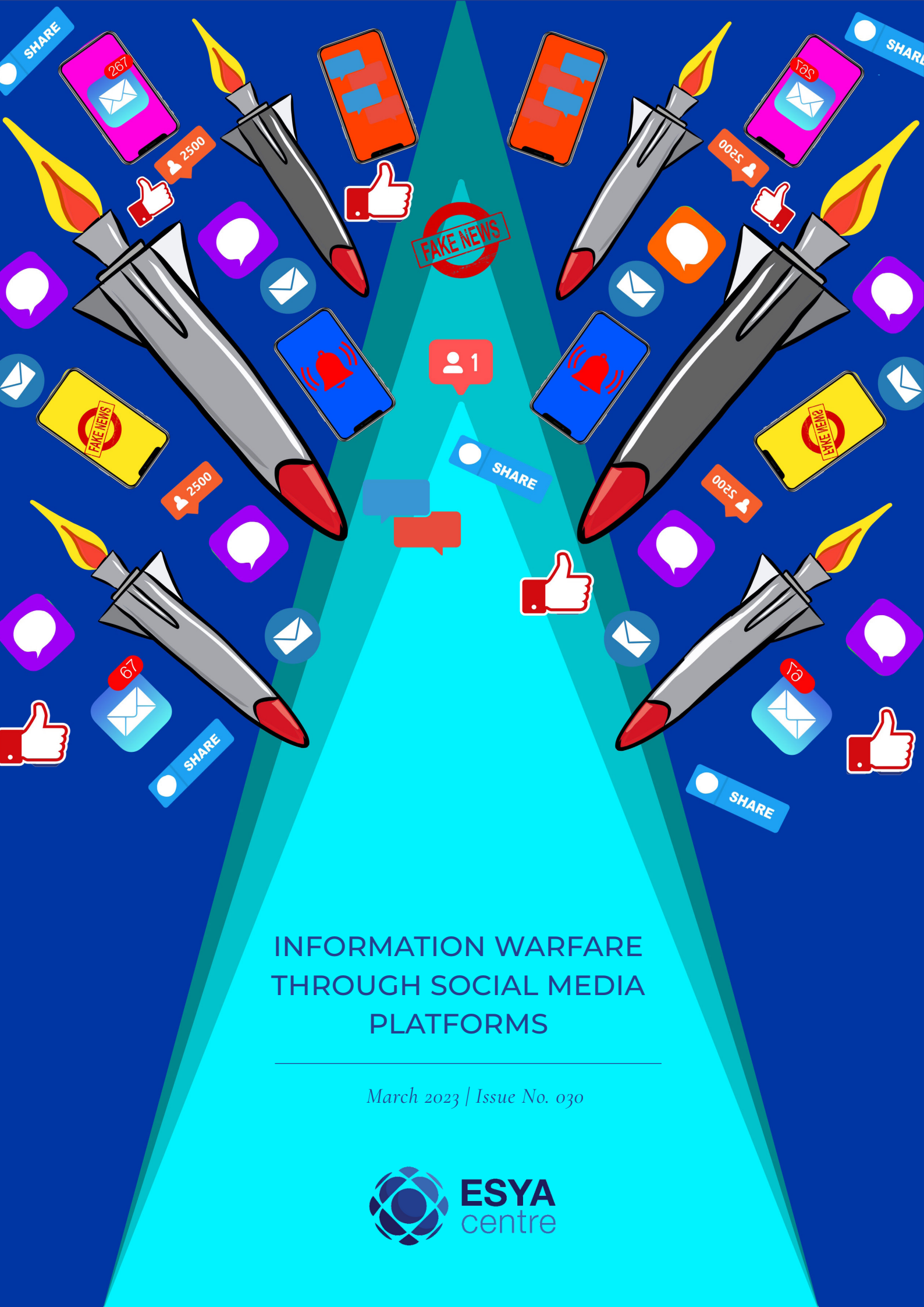

INFORMATION WARFARE THROUGH SOCIAL MEDIA PLATFORMS

March 2023 | Issue No. 030

ESYA centre

Attribution: Vaishnavi Prasad and Meghna Bal. *Information Warfare Through Social Media Platforms*. March 2023, Esya Centre.

Esya Centre
B-40 First Floor
Soami Nagar South,
New Delhi - 110017, India

The Esya Centre is a New Delhi based technology policy think tank. The Centre's mission is to generate empirical research and inform thought leadership to catalyse new policy constructs for the future. More details can be found at www.esyacentre.org.

About the Authors: Vaishnavi Prasad is a Research Assistant, and Meghna Bal is a Fellow at the Esya Centre.

Copyeditor: Aman Kumar

Cover Illustration: Taniya O'Connor

Layout & Design: Khalid Jaleel

CONTENTS

INTRODUCTION

The Russia-Ukraine conflict saw both countries use platforms such as Twitter, Facebook, Telegram, and TikTok to influence geopolitical dynamics and sway public opinion, highlighting the critical role that social media plays in armed conflict. However, information warfare isn't limited to instances of armed conflict alone. Today, in the information age, any organisation or even individuals can conduct information warfare to seize control of perceptions, and personal data.[1]

This paper focuses on information warfare operations conducted by foreign adversaries through social media platforms.[2] Specifically, it considers challenges related to social media and information warfare in the Indian context and makes suggestions on how India may mitigate such threats, in particular by leveraging and partnering with domestic social media platforms. The recommendations in the paper emanate from global best practices in responding to these threats.

Part I of the report defines the scope of the paper, and presents a typology of social media platforms that the report focuses on. Part II identifies the various components of information warfare on social media. This includes psychological operations, cyber warfare, and intelligence-based warfare. This section examines the aforementioned with the use of case-studies, the harms it is likely to cause, and the steps that must be taken to mitigate these threats. Part III identifies the global best practices in tackling information warfare. Part IV examines India's regulatory and institutional approaches to addressing this threat. Part V of the report presents a summary of recommendations.

1. Andrew Jones, *"Global Information Warfare: How Businesses, Governments, and Other Achieve Objectives and Attain Competitive Advantages"*, Auerbach Publications (2002).

2. For clarity, the term "foreign adversaries" includes the government, or military of a hostile foreign nation, persons or entities affiliated to a hostile foreign nation, or individuals who belong to malicious foreign groups.

I. UNDERSTANDING INFORMATION WARFARE BY FOREIGN ADVERSARIES THROUGH SOCIAL MEDIA

Although there is no unified definition of information warfare, it can broadly be described as any activity that seeks to *"steal, plant, interdict, manipulate, distort or destroy information."*[3] Going by this description, it is clear that any institution or individual can be party to information warfare.[4]

The involvement of civilians in information warfare has greatly been enhanced by the arrival of social media platforms that enable users to theoretically connect to networks of millions/billions of people.[5] These platforms also collect and process vast troves of metadata related to location, and personally identifiable information of users, which can be collated and parsed to generate insights that may have national security implications. For instance, location information has been used to generate heat maps of secret installations of military intelligence agencies.[6]

While several applications have a social component, the focus of this paper is on platforms where social networking is the central product on offer, i.e., internet-based channels of mass personal communications that let users participate in social networking and derive value primarily from user-generated content networking.[7] A broad categorisation of these platforms is as follows:

3. Giles, K., *"Handbook of Russian Information Warfare"*, NATO Defense College Research Division, (2016), https://www.ndc.nato.int/news/news.php?icode=995.

4. Andrew Jones, *"Global Information Warfare: How Businesses, Governments, and Other Achieve Objectives and Attain Competitive Advantages"*, Auerbach Publications (2002).

5. Christopher Whyte, Trevor Thrall, and Brian M. Mazanec, *"Information Warfare in the Age of Cyber Conflict"*, Routledge, (2020), https://doi.org/10.4324/9780429470509.

6. Alex Hern, *"Fitness tracking app Strava gives away location of secret US army bases"*, the Guardian, (28 January 2018), https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases

7. Caleb T. Carr, "Social Media: Defining, Developing, and Divining", Atlantic Journal of Communication, Volume 23, Issue 1 (2015), https://doi.org/10.1080/15456870.2015.972282; Miller D, Costa E, Haynes N, et al., "How the World Changed Social Media", UCL Press (2016),https://doi.org/10.2307/j.ctt1g69z35.

A. Micro-blogging platforms: Twitter and Koo

Twitter is a microblogging and social networking service where users can post text, photos, videos, and audio messages.[8] Users can engage with each other by replying to tweets, resharing content by retweeting it, and sharing it with a comment by quote-tweeting it. Tweets are grouped by hashtags. Twitter is also a messaging platform that allows users to message individuals and groups. Twitter also introduced a social audio feature called 'Spaces' that enables users to host or participate in live-audio virtual environments. They can accommodate an unlimited number of listeners.[9]

Koo is an Indian microblogging and social networking service.[10] Its user interface is similar to Twitter's, and lets users share 400-character updates, audio clips, photos, and videos. They can categorise their posts with hashtags, and tag other users in mentions and replies. Users can 're-koo', which is Koo's version of a retweet. It was introduced in Kannada but supports Hindi, English, Tamil, Telugu, Assamese, Marathi, Bangla, and Gujarati. It has different silos divided by language and the app is customised for the chosen language.

B. Multi-purpose social networking platforms: Facebook and Sharechat

Facebook is a social networking service owned by Meta,[11] where every user has a personal profile showing their posts and content. They can interact with posts made by other users by either reacting to them with an emoji, commenting, or sharing it. They can join groups and communities which may either be open or limited to certain people and personally message other users. Facebook also introduced its Pages feature for brands and organisations to interact with their followers.

Sharechat is a social networking site that consists of chat rooms and groups for a user to explore content.[12] These groups exist for a large number of subjects and interests. Sharechat also allows users to create and share photos

8. Twitter, www.twitter.com.

9. Twitter, "About Twitter Spaces", https://help.twitter.com/en/using-twitter/spaces#:~:text=the%20Spaces%20icon.-,You%20can%20also%20start%20a%20Space%20by%20selecting%20the%20Spaces,or%20sharing%20a%20link%20elsewhere

10. Koo, https://www.kooapp.com/.

11. Facebook, https://www.facebook.com/facebook/.

12. Sharechat, https://sharechat.com/.

and videos. It is a resource of short videos, jokes, gifs, and songs that users can download. It is available in around 15 regional languages. It also provides curated content that can be accessed by the user.

C. Messaging platforms: WhatsApp and Telegram

WhatsApp is an instant messaging service owned by Meta that allows users to message each other individually or through groups.[13] Whatsapp also offers audio calling and video calling services. Messages can be in the form of texts, photos, videos, or documents.

Telegram is another globally accessible instant messaging service,[14] very similar to WhatsApp, that offers a secret chat service through a client-to-client encryption software. This can be done only in those devices where a secret chat has been initiated and accepted by the users.

D. Short-form Video Hosting Platforms: TikTok and Moj

TikTok is a short-form video hosting platform that allows users to create, watch, and share 15-second videos.[15] It is owned by ByteDance Ltd., a Chinese technology company.

Moj is an Indian video-sharing social networking platform.[16] It is designed to be an alternative to Tik-Tok after its ban in 2020. It lets users share short videos of fifteen seconds to one minute along with special effects, emoticons, and stickers.

13. WhatsApp, https://www.whatsapp.com/.

14. Telegram, https://telegram.org/.

15. TikTok, https://www.tiktok.com/en/.

16. Moj, https://mojapp.in/.

II. COMPONENTS OF INFORMATION WARFARE ON SOCIAL MEDIA

Libicki has defined the parameters of information warfare by identifying seven of its major components: command and control warfare, intelligence warfare, electronic warfare, psychological operations, hacker warfare, economic information warfare, and network/cyber warfare.[17] This categorization has also been reflected in the works of Brazolli,[18] Shallcross[19] and Van Niekerk.[20]

However, Shallcross, in the context of information warfare through social media, deems the following components relevant:

A. Psychological Operations

Psychological operations seek to alter the perceptions of the audience to be favourable to one's objectives. Deception, information disorder, and propaganda are some examples of psychological operations.[21] Information disorder consists of disinformation, misinformation and mal-information. Disinformation is inaccurate information that is intentionally spread to mislead.[22] Misinformation is inaccurate information that is innocuously

17. Martin Libicki, *"What is Information Warfare?"*, Strategic Forum Number (28, May 1995), https://apps.dtic.mil/sti/citations/ADA367662.

18. Brazzoli, M. S., *"Future prospects of information warfare and particularly psychological operations"*, South African Army Vision 2020, Institute for Security Studies, Pretoria, (2007).

19. Shallcross, *"Social Media and Information Operations in the 21st Century"*, Journal of Information Warfare, Volume 16(1), (2017), https://www.jinfowar.com/journal/volume-16-issue-1/social-media-information-operations-21st-century.

20. Van Neikerk et. al., *"Social Media and Information Conflict"*, International Journal of Communication, Volume 7, (23, May 2013), https://ijoc.org/index.php/ijoc/article/view/1658/919.

21. Bates, Rodger A., and Mara Mooney. *"Psychological operations and terrorism: The digital domain"*, Volume 6 Issue 1, The Journal of Public and Professional Sociology, (2014), https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=1070&context=jpps.

22.Shu, Kai, et al. "Mining disinformation and fake news: Concepts, methods, and recent advancements." *Disinformation, misinformation, and fake news in social media*. Springer, Cham, (2020), Shu, Kai, et al. "Mining disinformation and fake news: Concepts, methods, and recent advancements." *Disinformation, misinformation, and fake news in social media*. Springer, Cham, 2020. 1-19.

shared by a person without the intent to deceive.[23] Malinformation is accurate information shared with the intent to cause harm.[24]

1. Harms of psychological operations

i. Interferes with the democratic discourse of a country

Psychological operations in the form of social media information campaigns and propaganda allow foreign adversaries to interfere in domestic discourse. Various social media platforms provide these adversaries with the tools they need to strategically insert false narratives in order to mislead the public and skew the outcomes of democratic discourse.[25] Malicious groups may also employ coordination tactics to amplify misleading narratives and manipulate public opinion at an unprecedented scale.[26]

This was seen in the large-scale propaganda campaigns on Twitter after Russia invaded Ukraine earlier this year.[27] A study by Dominique Geissler et. al. examined 349,455 messages on Twitter between February and July 2022 with pro-Russian content. It revealed that Russia launched a systematic, coordinated propaganda campaign which reached around 14.4 million users.[28]

The massive reach of this propaganda can be attributed to the low cost of producing high volumes of bots with the cost of a single bot being less than $1.[29] Bots amplify misinformation by spreading low-credibility content at the early stages. Consequently, they are likely to shape online discourse and

23. Id.

24. Id.

25. Christopher Whyte and Ugochukwu Etudo, *"Cyber by a Different Logic, Using an information warfare kill chain to understand cyber-enabled influence operations"* in *"Information Warfare in the Age of Cyber Conflict"*, Routledge, (2020), https://doi.org/10.4324/9780429470509.

26. Pacheco et. al., *"Uncovering Coordinated Networks on Social Media: Methods and Case Studies"*, Volume 15, Fifteenth International AAAI Conference on Web and Social Media, (2021), https://arxiv.org/pdf/2001.05658.pdf.

27. John Psaropoulos, *"Timeline: Six months of Russia's war in Ukraine"*, Al Jazeera, (24 August 2022), https://www.aljazeera.com/news/2022/8/24/timeline-six-months-of-russias-war-in-ukraine.

28. Geissler, D., Bär, D., Pröllochs, N. and Feuerriegel, S., *"Russian propaganda on social media during the 2022 invasion of Ukraine"*, 2022, arXiv preprint arXiv:2211.04154.

29. CB Insights, "Disinformation That Kills: The Expanding Battlefield Of Digital Warfare", (21 October, 2020), https://www.cbinsights.com/research/future-of-information-warfare/

radicalise users.[30] This can be evidenced by the fact that these tweets have not only received over 251,000 retweets, but also are being created and shared in different languages.

Similarly, in India, after in clash in Galwan in 2020 that resulted in the deaths of 20 Indian soldiers, there was a psychological operation conducted by Pakistan with around 400-500 Twitter accounts spreading false narratives in favour of China.[31] Therefore, these campaigns by foreign adversaries are likely to influence public opinion in a manner that is detrimental to national interest.

ii. Psychological operations threaten the integrity of a nation's elections

Psychological operations by foreign adversaries that aim at spreading propaganda and influencing public debates can affect the outcome of elections in a country. For instance, in 2016, prior to the Brexit referendum, Russia launched an extensive pro-Brexit campaign on social media platforms such as Twitter by using thousands of bots.[32] Over four hundred accounts were used to circulate disinformation in the weeks leading to the referendum.[33] There is no literature to prove that these operations definitively influenced the outcome.[34] However, the narrow margin of victory of the Leave campaign (51.89%) as well as the pervasive influence of social media in shaping political opinions indicate that these operations may have been a significant factor. Further, research has been undertaken in the context of other psychological operations by Russia to prove their intent to interfere in the elections and

30. Massimo Stella et. al., *"Bots increase exposure to negative and inflammatory content in online social systems"*, Proceedings of the National Academy of Sciences of the United States of America, (2018), https://doi.org/10.1073/pnas.1803470115.

31. Prateek Goyal and Anna Priyadarshini, *"How a "disinformation network" on Twitter added to the tension surrounding the Galwan Valley conflict"*, Newslaundry, (2020), https://www.newslaundry.com/2020/07/18/how-a-disinformation-network-on-twitter-added-to-the-tension-surrounding-the-galwan-valley-conflict

32.Galante, Laura, and Shaun, *"Defining Russian Election Interference: An Analysis of Select 2014 to 2018 Cyber Enabled Incidents"*, Atlantic Council, (2018),, http://www.jstor.org/stable/resrep20718.

33. Robert Booth, Matthew Weaver, Alex Hern, Stacee Smith and Shaun Walker, *"Russia used hundreds of fake accounts to tweet about Brexit, data shows,"* The Guardian, (2017), https://www.theguardian.com/world/2017/ nov/14/how-400-russia-run-fake-accounts-posted-bogus-brexit-tweets.

34. Intelligence and Security Committee of Parliament, *"Russia"*, (2020), See https://isc.independent.gov.uk/wp-content/uploads/2021/03/CCS207_CCS0221966010-001_Russia-Report-v02-Web_Accessible.pdf.

democratic processes of various countries.[35] For instance, the US released an Intelligence Community Assessment report that established that the Russian-led influence campaign targeted the US Presidential election in 2016 with the aim of undermining public faith in the electoral process and harming the electability of Secretary Clinton.[36]

iii. Foreign adversaries can use psychological operations to recruit and mobilise individuals (command and control warfare)

Social media enables foreign adversaries to recruit supporters and direct operations from remote locations. This is known as command and control warfare. [37] Facebook's basic principles of data mining and analysis, profiling, personalizing, targeting, and encouraging sharing has been effectively used by the Islamic State of Iraq and Syria ("ISIS") to influence, recruit, and direct vulnerable individuals to the West to conduct terrorist attacks. ISIS routinely creates high-quality, emotionally evocative propaganda videos and ideological content in several different languages across the world which enables them to recruit foreign terrorist fighters (FTFs). [38] ISIS has also relied on Telegram to disseminate propaganda and recruit individuals to conduct lone-wolf terrorist attacks, carried out by individuals who do not belong to an organized terrorist group.[39] Telegram's channel feature that allows the creation of public and private channels enabled ISIS to create several channels in various languages and create ad-hoc networks.[40] Propaganda materials that

35. Erik Brattgerg and Tim Maurer, *"Five European Experiences with Russian Election Interference, Carnegie Endowment for International Peace"*, (2018), https://carnegieendowment.org/2018/05/23/russian-election-interference-europe-s-counter-to-fake-news-and-cyber-attacks-pub-76435.

36. Intelligence Community of America, *"Assessing Russian Activities and Intentions in the Recent US Elections"*, (2017), https://www.intelligence.senate.gov/sites/default/files/documents/ICA_2017_01.pdf

37. Shallcross, *"Social Media and Information Operations in the 21st Century"*, Journal of Information Warfare, Volume 16(1), (2017), https://www.jinfowar.com/journal/volume-16-issue-1/social-media-information-operations-21st-century.

38. Matteo Vergani and Ana-Maria Bliuc, "The Evolution of the ISIS' Language: A Quantitative Analysis of the Language of the First Year of Dabiq Magazine," Sicurezza, Terrorismo e societa, (2015), https://discovery.dundee.ac.uk/en/publications/the-evolution-of-the-isis-language-a-quantitative-analysis-of-the,

39. Ramon Spaaij, *"The Enigma of Lone Wolf Terrorism: An Assessment,"* Studies in Conflict and Terrorism, Volume 33, Issue 9, (2010), https://doi.org/10.1080/1057610X.2010.501426.

40. Ahmed Shehabat, Teodor E. Mites, Yehia Alzoubi, *"Encrypted Jihad: Investigating the Role of the Telegram App in Lone Wolf Attacks in the West"*, Journal of Strategic Security, Volume 110, Issue 3, (2017), https://ro.uow.edu.au/cgi/viewcontent.cgi?article=4324&context=lhapapers.

seek to recruit individuals to conduct lone wolf attacks and join ISIS are initially released on these channels. Subsequently, they are disseminated on platforms like Twitter.[41]

41. J.M. Berger and Heather Perez, *"The Islamic State's Diminishing Returns on Twitter: How suspensions are limiting the social networks of English-speaking ISIS supporters"*, https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/Berger_Occasional %20Paper.pdf

2. *Psychological operations on domestic social media platforms*

Psychological operations in India are not only limited to platforms like Facebook and Twitter but are likely to extend to domestic social media platforms such as Sharechat and Koo.[42] Indian social media platforms such as Sharechat, Koo, and Moj see hundreds of millions of monthly active users. Their rapidly growing user bases increase the likelihood of foreign adversaries utilising these platforms to conduct psychological operations. These platforms normally employ an algorithm to analyse words, phrases and hashtags in order to create a "trend list" of the most popular topics. Consequently, foreign adversaries can hijack these trend lists with their own agenda by creating and disseminating messages swiftly with bots.[43]

B. Network Warfare

Network warfare has been defined as the offensive and defensive actions that relate to information, communications, and computer networks and infrastructure.[44] Users are more vulnerable to cyber-attacks in social media platforms than in traditional web pages. This is because its design allows users to upload and share media as well as interact with each other. All these increase the likelihood of malicious code and software being shared to a user without their knowledge. [45] Social media can be utilised by foreign adversaries to exploit vulnerabilities in a user's software and obtain access to their sensitive information.[46]

---

42. See India News, *"Fake news and hate speech thrive on regional language social media"*, Hindustan Times, (2018), https://www.hindustantimes.com/opinion/how-regional-social-media-platforms-spew-fake-news-and-get-away-with-it/story-s8Kc2s4TKfneoZRlXNuLuM.html

43. Lt Col Jarred Prier, USAF, *"Commanding the Trend: Social Media as Information Warfare"*, Strategic Studies Quarterly, (2017), https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-11_Issue-4/Prier.pdf.

44. Shallcross, "*Social Media and Information Operations in the 21st Century*", Journal of Information Warfare, Volume 16(1), (2017), https://www.jinfowar.com/journal/volume-16-issue-1/social-media-information-operations-21st-century.

45. Lawton, "*Web 2.0 creates security challenges*", Computer, Volume 40 Issue 10, (2007), https://www.computer.org/csdl/magazine/co/2007/10/mco2007100013/13rRUxjyXdN; Van Neikerk et. al., "*Social Media and Information Conflict*", International Journal of Communication, Volume 7, (23, May 2013), https://ijoc.org/index.php/ijoc/article/view/1658/919..

46. Shallcross, "*Social Media and Information Operations in the 21st Century*", Journal of Information Warfare, Volume 16(1), (2017), https://www.jinfowar.com/journal/volume-16-issue-1/social-media-information-operations-21st-century.

1. Network warfare threats on social media platforms

i. Spear phishing

Spear phishing campaigns are undertaken by seeding a list of accounts in a social media platform into a program. Then the program generates customised messages based on the content of their social media profiles along with a malicious link and sends it directly to the target. Once the target clicks the link, it installs malware into a user's device and compromises its security. This malware can lead victims to fabricated websites that ask for certain login credentials which then are utilised to gain access to a broader network of information.[47] For instance, in 2016, over 10,000 tweets with hyperlinks containing malware were sent directly to employees of the U.S. Defence Department. The messages in the tweets were tailored to appeal to the person they were sent to and devices containing sensitive government information were compromised.[48] Similarly, in 2020, North Korean hackers posing as employees of large US military contractors compromised the systems of defence and aerospace firms in Central Europe by disseminating fake job offers on LinkedIn.[49] Domestic social media platforms that allow users to message each other are inevitably vulnerable to spear phishing attempts by foreign actors.

ii. Data Breaches

A data breach occurs when a company's security is compromised, resulting in a breach of the confidentiality, availability, and integrity of data.[50] Over the past few years, there have been several large-scale data breaches that have involved some prominent social media platforms. In 2022, Twitter[51]

47. Michael Bossetta, *"The weaponization of Social Media: Spear Phishing and Cyberattacks on Democracy"*, Journal of International Affairs, Volume 71, Issue 1.5, (2018), https://lucris.lub.lu.se/ws/portalfiles/portal/85420559/The_Weaponization_of_Social_Media_Bossetta_2018_.pdf

48. Massimo Calabresi, *"Inside Russia's Social Media War on America,"* Time, (2017), https://time.com/magazine/us/4783906/may-29th-2017-vol-189-no-20-u-s/.

49. Min Chao Choy & Nils Weisensee, "North Korean hackers targeted aerospace, defence companies via LinkedIn: experts", NkNews, (2020), https://www.nknews.org/2020/06/north-korean-hackers-targeted-aerospace-defense-companies-via-linkedin-experts/.

50. European Commission, *"What is a data breach and what do we have to do in case of a data breach?"*, https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-data-breach-and-what-do-we-have-do-case-data-breach_en.

51. Olivia Powell, *"Twitter confirms data from 5.4 million accounts has been stolen"*, (2022), https://www.cshub.com/attacks/news/twitter-confirms-data-from-54-million-accounts-has-been-stolen.

and Facebook[52] have had data breaches that exposed the personal data of millions of users. Social media platforms that place inadequate emphasis on cybersecurity leave users vulnerable to cyberattacks that result in having their personal information exposed. For instance, in 2021, a French cyber expert identified security loopholes in Koo that could be misused to retrieve personally identifiable information.[53]

iii. Distributed denial-of-service attacks (command and control warfare)

Foreign adversaries seek to disrupt the ability of their target's forces to coordinate and mobilise. This is another facet of command and control warfare.[54] Disruptive command and control warfare has been utilised by Chinese hackers in Hong Kong. Telegram's end-to-end encryption feature was used by individuals in Hong Kong protesting against China's proposed Fugitive Offenders Ordinance that would enable criminal suspects to be sent to Mainland China for trial. They protested on the grounds that the ordinance was a convenient tool to suppress dissent against the Communist Party of China. As protests intensified, Chinese hackers launched DDoS attacks where the servers were flooded with junk communications at 200-400 gigabits per second. These attacks used bots that attempted to cause Telegram's server to malfunction by flooding it with malicious communications, thus rendering it inaccessible.[55]

2. *Harms of Network Warfare*

i. Sensitive information systems are compromised

Spear phishing attacks target individuals with customised messages such that they are incentivised to click on the media containing malware. This malware is likely not only to compromise the victim's personal information on the social media platform, but also the device they are accessing the platform from. This is particularly dangerous when it comes to high profile individuals

52. Eray Eliacik, "*Facebook Data Breach 2022: Over 1M users affected*", Data Economy, https://dataconomy.com/2022/10/facebook-data-breach-2022/.

53. Rohit KVN, "*French cyber expert shows data leak on Koo app, company denies any breach*", Deccan Herald, (2021), https://www.deccanherald.com/specials/french-cyber-expert-shows-data-leak-on-koo-app-company-denies-any-breach-949976.html

54. Shallcross, "*Social Media and Information Operations in the 21st Century*", Journal of Information Warfare, Volume 16(1), (2017), https://www.jinfowar.com/journal/volume-16-issue-1/social-media-information-operations-21st-century.

55. Jonathan Shieber, "*Telegram faces DDoS attack in China... again*", TechCrunch (2019), https://techcrunch.com/2019/06/12/telegram-faces-ddos-attack-in-china-again/.

in the government or military, as foreign adversaries may access sensitive data pertaining to national security.

ii. Foreign adversaries can exploit the personal data of citizens

Data breaches can result in foreign adversaries obtaining access to a wide range of personal data such as contact details, address, marital status, and sexuality, among others. This information can be used to launch targeted psychological operations or sophisticated phishing attacks. It can also be used by terrorist organisations to recruit and organise individuals more effectively.

C. Intelligence-Based Warfare: Foreign investments, mergers, and acquisitions

Information warfare is not only the use or dissemination of information, it also includes the process of obtaining that information in the first place.[56] Intelligence-based warfare is defined as actions taken by an adversary to degrade one's intelligence cycle.[57] This involves intelligence gathering and compromising information sources and systems. Foreign investments, mergers, and acquisitions of domestic social media platforms pose as a likely intelligence-based warfare threats for two reasons: *One,* foreign actors are likely to get access to the personal data of citizens, posing a threat to the national security of a country[58]; and *two,* ownership will allow them to exercise more control over the kind of content being disseminated in these platforms.

56. Castells, Manuel, "*Communication power,*" Oxford: Oxford University Press, 2013.

57. Shallcross, "*Social Media and Information Operations in the 21st Century*", Journal of Information Warfare, Volume 16(1), (2017), https://www.jinfowar.com/journal/volume-16-issue-1/social-media-information-operations-21st-century.

58. See CFIUS opposition to Bytedance's acquisition of Musical.y in CSIS, "*TikTok Is Running out of Time: Understanding the CFIUS Decision and Its Implications*", available at: https://www.csis.org/analysis/tiktok-running-out-time-understanding-cfius-decision-and-its-implications.

III. GLOBAL BEST PRACTICES

A. Psychological Operations

1. Regulatory Approaches

i. Singapore: Defining and penalising foreign interference in democratic discourse

Singapore's Foreign Interference (Countermeasures) Act provides measures to prevent, detect and disrupt foreign interference in Singapore politics through hostile information campaigns. This Act defines foreign interference as any action undertaken by or on behalf of a foreign principal or a person acting on behalf of a foreign principal.[59] This Act penalises clandestine foreign interference by electronic communications activity in a variety of situations. Some such situations include promoting the interests of a political party, to influence or seek to influence the outcome of any election or national referendum, Singapore government decisions, or parliament proceedings, and communications that are likely to diminish public confidence in the performance of the Government or a public authority.[60]

The legislation provides comprehensive definitions of foreign interference, influence towards a political end, and what constitutes social media publication. However, one caveat that comes with this wide-ranging definition is that without adequate safeguards, it could stifle political dissent and cause a chilling effect on free speech.[61]

ii. Australia: Penalising foreign interference

In 2018, Australia amended its criminal codes to include a foreign influence transparency scheme and offences pertaining to foreign interference. Here, foreign influence is differentiated from interference in the following manner: interference is when actions are directed by, on behalf or, or in collaboration with a foreign power in a manner that is detrimental to the

59. Section 6, Singapore, Foreign Interference (Countermeasures) Act, https://sso.agc.gov.sg/Acts-Supp/28-2021/Published/20211125?DocDate=20211125.

60. Section 9, Section 17, Section 18, Singapore, Foreign Interference (Countermeasures) Act.

61. https://www.bbc.com/news/world-asia-58798373

country's interests.[62] Whereas, influence is considered to occur in an open and transparent manner and is a part of usual diplomacy.

The Act penalises foreign interference. This includes intentional and reckless foreign interference as well as preparing for or planning foreign interference. The interference must be likely to influence a political or government process, or the exercise of a democratic or political right, or must prejudice the national security of the country.[63] These provisions are applicable to conduct that occurs beyond the borders of Australia but the results of which are present within Australia.[64]

However, these provisions have also been criticised for their overarching ambit and potential to threaten journalistic freedom. Some recommendations that have been made include clearly defining what constitutes a prejudice to national security, and including a good-faith journalism based exemption from criminal liability.[65]

iii. Ireland: Penalising the usage of bots

Ireland's Online Advertising and Social Media Transparency Bill, 2017 penalises the usage of bots to cause multiple online presences directed towards a political end. It defines bots as any software that is programmed to run automated tasks online.[66] Further, matters directed towards political ends are defined as those that promote certain candidates during an election or certain messages on matters of political interest. It also includes matters that are either before or intended to be presented before legislative and judicial authorities.[67]

62. 'Director-General's Annual Threat Assessment', Australian Security Intelligence Organisation (Speech, 17 March 2021)

63. Section 92.3, National Security Legislation Amendment (Espionage and Foreign Interference) Act, 2018, https://www.legislation.gov.au/Details/C2018A00067.

64. Id. at Section 92.6.

65. Sarah Kendall, "*How Australia's Foreign Interference Laws Undermine Press Freedom*", Alternative Law Journal, Vol 47(2), 2022, 124-129.

66. Section 2(1), Online Advertising and Social Media (Transparency) Act, 2017 (Ireland).

67. Id.

iv. EU and Australia: Private Sector responses

On the regulatory front, the European Union introduced the Code of Practice on Disinformation.[68] This Code was monumental because for the first time worldwide, industries agreed, on a voluntary basis, to self-regulatory standards to combat disinformation. It has been signed by platforms such as Meta, Google, Twitter, Mozilla, Microsoft, and TikTok.[69] The signatories committed to include safeguards against disinformation, demonstrate the effectiveness of efforts to close fake accounts and establish clear marking systems and rules for bots to ensure that their activities cannot be confused with human interactions, and promote transparency in political advertisements. This Code was strengthened earlier this year, in 2022, to include information influence operations and foreign interference in the information space. [70]

A similar initiative in Australia was undertaken by the Digital Industry Group, a non-profit industry association that advocates for the interests of the digital industry in Australia. They introduced the Australian Code of Practice on Disinformation and Misinformation.[71] This Code has been signed by various digital platforms to affirm their minimum commitments towards fighting information disorder. The Code recommends that platforms introduce policies that require human review of user behaviours, labelling false content or providing trust indicators of content to users, and ensure transparency on their efforts to address information disorder.[72]

68. European Union, *"2018 Code of Practice on Disinformation"*, https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation.

69. European Commission, *"2018 Code of Practice on Disinformation"*, (2022), https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation.

70. European Union, *"The Strengthened Code of Practice on Disinformation, 2022"*, https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation.

71. Digital Industry Group Inc., *"Australian Code of Practice on Disinformation and Misinformation"*, (2021), https://digi.org.au/wp-content/uploads/2021/02/Australian-Code-of-Practice-on-Disinformation-and-Misinformation-FINAL-PDF-Feb-22-2021.pdf

72. Paragraph 5.9, Australian Code of Practice on Disinformation and Misinformation.

2. *Institutional approaches*

i. Australia and UK: Electoral Integrity Task Forces

The UK established the National Cyber Force in 2020 with the objective of identifying and tackling threats to the UK and promoting UK interests.[73] This task force is composed of personnel from defence and intelligence. One of the goals of this task force is to defend democracy, free, fair, and open elections by countering state disinformation campaigns intended to undermine them.

Yet another endeavour to safeguard free, fair, and open elections is Australia's Electoral Integrity Assurance Task Force.[74] The role of this entity is to provide advice to the Australian Election Commission regarding cyber interference with the electoral process. While their primary concern is cybersecurity, they also monitor the potential use of disinformation and messaging, and any other information operation that seeks to disrupt elections.

ii. US' Joint Defense Collaborative: Public-Private Partnerships

The US's Cyber Infrastructure and Security Agency has partnered with several technology companies under its Joint Cyber Defense Collaborative. They coordinate cyber defence planning and execution through collaborative public-private sector cybersecurity, information sharing, fusion, and analysis. For instance, they developed a Russia-Ukraine Tensions Plan that laid down the phases of coordination between the US Government and private sector partners.

iii. Private Sector Initiative: The Global Internet Forum to Counter Terrorism

The Global Internet Forum to Counter Terrorism is an initiative founded by Facebook, Microsoft, Twitter and Youtube to facilitate resource sharing in order to counter terrorist and violent extremist activity online. [75] The three pillars of this forum are: *One,* the preventing terrorist and extremist activity online by equipping platforms with the requisite knowledge and tools; *two,* mitigating the impact of a terrorist attack by bringing together relevant stakeholders; and *three,* knowledge building by supporting research in the intersection of terrorism and technology.

73. Government, UK, *"About Us, National Cyber Force"*, https://www.gov.uk/government/organisations/national-cyber-force/about.

74. Australian Government, *"Electoral Integrity Assurance Taskforce"*, https://www.aec.gov.au/about_aec/electoral-integrity.htm

75. Global Internet Forum to Counter Terrorism, https://gifct.org/

B. Network Warfare

1. Legislative approaches: EU: The GDPR Penalising Data Breaches

According to the GDPR, in the event of a personal data breach, the responsible organisation must notify the relevant supervisory authority within 72 hours of having become aware of it.[76] When the data breach poses a high risk to affected individuals, they must be informed.[77] However, if there are effective technical and organisational measures in place to ensure that the risk is not likely to materialise, the data subjects need not be informed.[78]

Further, the GDPR mandates that the organisation shall implement the appropriate technical and organisational measures to ensure an appropriate level of security such that personal data is not made accessible to unauthorised persons.[79] Some measures they may incorporate include the pseudonymisation and encryption of personal data, and regular assessment of the effectiveness of technical and organisational measures to protect personal data.[80] Violation of these provisions can lead to steep penalties.[81] For instance, the Irish Data Protection Commission fined Meta platforms 265 million euros after a data breach that resulted in the personal details of millions of Facebook users leaked.[82]

i. EU Cyber Defence Policy

On 10th November, 2022, the European Commission and the High Representative published a Joint Communication on an EU Cyber Defence Policy to address the deteriorating security environment in light of the Ukraine-Russia conflict.[83] The Communication acknowledged how cyber-attacks are often cross-border and hybrid where disinformation campaigns

76. Article 33, General Data Protection Regulation ("GDPR").

77. Article 34, GDPR.

78. Id.

79. Article 25, GDPR.

80. Article 32, GDPR.

81. Article 83, GDPR.

82. BBC "*Facebook: Meta fined 265 million euros by Irish Data Protection Commission*", (2021) https://www.bbc.com/news/world-europe-63786893

83. See European Union Institute for Security Studies, "A Language of Power? Cyber defence in the European Union", (2022), https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_176_0.pdf.

are combined with cyber-attacks on infrastructure with the potential for obtaining unlawful access to sensitive data.[84] Some recommendations made to address these issues are: (i) securing the EU defence ecosystem by enhancing its cyber resilience and ensuring it is interoperable and has coherence of standards; (ii) investing in cyber defence capabilities and developing a full-spectrum state-of-the-art defence; and (iii) partnering with entities like NATO to address common challenges in cyber security. This can also involve cyber defence capacity building support for partner countries.[85]

2. *Institutional approaches: US's Cybersecurity and Infrastructure Security Agency and Finland's Comprehensive Security*

US's Cybersecurity and Infrastructure Security Agency is the federal agency that identifies, manages, and reduces risk to the country's cyber and physical infrastructure. They do so by collaborating with relevant stakeholders in the industry and facilitating them in building cyber resilience.[86] In 2021, CISA launched the Joint Cyber Defense Collaborative where they collaborated with 15 of the country's largest cybersecurity, technology, and infrastructure companies. For instance, Log4Shell is a vulnerability impacting multiple versions of Apache Log4j library, an open-source Java package that is used by developers across the world.[87] Log4Shell enables malicious actors to take advantage of this and target vulnerable servers. Once the JCDC was made aware of this, they shared indicators of compromise, threat activity and intelligence with its members in order to enable them to swiftly take action on the same. [88] Similarly, Finland's Comprehensive Security Model aims to create collaboration between the authorities and other relevant stakeholders in the fields of research and development, and the exchange of information with mutual coordination.[89]

84. European Commission, "Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade", JOIN(2020)18 final, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020JC0018&from=ga.

85. Id.

86. About CISA, https://www.cisa.gov/about-cisa

87. Singapore Computer Emergency Response Team, *"The Log4Shell Vulnerability"*, (2022), https://www.csa.gov.sg/singcert/Publications/the-log4shell-vulnerability

88. CISA, *"Apache Log4j Vulnerability Guidance"*, https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance

89. Turvallisuuskomitea Sakerhetskommitten, *"Comprehensive Security"*, https://turvallisuuskomitea.fi/en/comprehensive-security/.

i. EU's Cyber Rapid Response Teams and Mutual Assistance in Cyber Security

Lithuania coordinated the Cyber Rapid Response Teams and Mutual Assistance in Cyber Security (CRRTs) along with other EU members in order to help each other ensure a higher level of protection against cyber incidents as well as collectively respond to them.[90] CRRTs are normally equipped with a common cyber toolkit that will enable them to detect, recognise, and mitigate cyber threats. Experts in cybersecurity from the participating member states would assist each other with training and vulnerability assignments.[91]

C. Intelligence-Based Warfare

1. The Committee on Foreign Investment in the United States and the Foreign Investment Risk Review Modernisation Act

Section 721 of the US Defence Production Act, 1950 gives authority to the Committee on Foreign Investment in the United States (CFIUS) to review certain mergers, acquisitions, and takeovers that may have implications for national security.[92] In essence, CFIUS is an inter-agency committee that aids the US President in checking national security risks posed by Foreign Direct Investment.[93] Specifically, on the basis of reports and analysis prepared by CFIUS, the US President can "block or suspend proposed or pending" foreign investment transactions with national security implications.

In 2018, US Congress passed the Foreign Investment Risk Review Modernisation Act (FIRRMA), which broadened the purview of CFIUS reviews to, among other things, transactions involving:[94] *One,* any noncontrolling investment in certain US businesses involved in critical technology, critical infrastructure, or collecting sensitive personal data on US citizens; and *two,* transactions in which a foreign government has a direct or indirect substantial interest.

90. Permanent Structured Cooperation (PESCO), "Cyber Rapid Response Teams and Mutual Assistance in Cyber Security", https://www.pesco.europa.eu/project/cyber-rapid-response-teams-and-mutual-assistance-in-cyber-security/.

91. Id.

92. FEMA, "The Defense Production Act of 1950, as Amended", (2018), https://www.fema.gov/sites/default/files/2020-03/Defense_Production_Act_2018.pdf

93. Id.

94. U.S. Department of the Treasury, *"The Committee on Foreign Investment in the United States"*, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius

Since the passage of FIRRMA, US Presidents have issued multiple executive orders with a key focus around security concerns around the involvement of foreign adversaries in social media and other information and communication technology applications:

1. In 2019, President Donald Trump issued an Executive Order on Securing the Information and Communications Technology Services Supply Chain (EO 13873) which created a mandate for the US Department of Commerce to head off national security risks that may arise from transactions involving foreign adversaries in the information and communication technology and services sector.[95] The Trump administration used EO 13873 as the basis to issue EOs 13942 and 13943 to ban TikTok and WeChat, two Chinese social media applications, respectively.[96]

2. In 2020, President Trump issued an order forcing Tiktok's parent company, ByteDance to divest its holdings in TikTok, on the basis of a CFIUS investigation.[97]

3. In March 2021, the Department of Commerce issued an interim final rule for the "assessment of national security risks arising from the ability of "foreign adversaries" to collect personal data and sensitive business data from the United States through software apps.[98] The Department of Commerce has issued multiple subpoenas to companies from certain countries in pursuit of this order.[99]

4. In 2021, the Biden administration issued an Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries (EO 14034). It directed the Department of Commerce to work in conjunction with the US Department of Homeland Security and the Director of National Intelligence to identify existing and emerging threats and

95. Wiley, *"Biden Administration revokes Trump EOs targeting TikTok, WeChat, and Other Chinese Software Apps; Initiates Broader Investigations into Software Apps by Foreign Adversaries"*, (2021), https://www.wiley.law/alert-Biden-Administration-Revokes-Trump-EOs-Targeting-TikTok-WeChat-and-Other-Chinese-Software-Apps-Initiates-Broader-Investigations-into-Software-Apps-by-Foreign-Adversaries

96. Id.

97. Id.

98. Id.

99. Id.

prepare recommendations for the White House to tackle them. The EO also revoked the EOs 13873, 13942, and 13943.[100]

5. In September 2022, President Biden issued an Executive Order for Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States (EO 14083).[101] EO 14083 provides guidance to CFIUS to consider additional factors in its reviews of mergers with national security implications.[102] These include transactions, even incremental ones, that can lead to loss of control of a US company over critical technology or give access to the sensitive personal data of US citizens to foreign adversaries.

Till date, the US President has only blocked five transactions using CFIUS, indicating that it is relied upon as a measure of last resort. However, the broadening of CFIUS' ambit to transactions involving sensitive personal data, coupled with requirement to look into incremental investments, in the recent Biden EO indicate that it is likely more transactions will be blocked in the coming years. Most recently, there have been calls for a CFIUS review of Elon Musk's acquisition of Twitter. Musk brought on a number of foreign investors to finance the transaction, some of whom the US deems adversaries.[103]

100 .Id.

101 . Executive Order 14083, *"Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States",* https://public-inspection.federalregister.gov/2022-20450.pdf

102 .Id.

103 . Sanjay Patnaik, "The national security grounds for investigating Musk's Twitter acquisition", Brookings, (2022), https://www.brookings.edu/research/the-national-security-grounds-for-investigating-musks-twitter-acquisition/; See also United States Senate, https://www.murphy.senate.gov/imo/media/doc/103122lettertocfiusretwitter.pdf.

IV. INDIAN APPROACHES

A. Psychological Operations

1. *India's legal framework to combat psychological operations is inadequate*

India does not have a legislation that addresses psychological operations by foreign actors. While both the Information Technology Act, 2000[104] and the Indian Penal Code, 1860[105] have provisions that permit its extraterritorial application on foreign actors, there aren't any provisions that pertain to psychological operations. Existing penal provisions criminalise certain forms of speech (for example, that which amounts to sedition[106], and promotes enmity between different communities on the grounds of religion, race, and place of birth among others).[107] With regard to content moderation on social media, the Intermediary Guidelines and the Digital Media Ethics Code, 2021 prescribes that social media platforms must inform their users to not share content that threatens the unity, security and sovereignty of India, is patently false and untrue, or is written in a form with the intent to mislead or harass.[108] However, there aren't any provisions that penalise the dissemination of disinformation on social media platforms.

2. *Internet shutdowns do not effectively tackle psychological operations*

The most common approach by the Indian Government to tackle instances of widespread misinformation on social media is through internet shut-downs. Until 2017, this was ordered by district magistrates under Section 144 of the Code of Criminal Procedure, 1973. In 2017, the Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules were issued.[109] These rules authorise the Secretary to the Government of India in the Ministry of Home Affairs or the Secretary to the State Government in-charge of the

104. Section 1(2), Information Technology Act, 2000.

105. Section 4, Indian Penal Code, 1860.

106. Section 124A, Indian Penal Code, 1860.

107. Section 153A, Indian Penal Code, 1860.

108. Rule 3(1)(b)(x), IG DME Code

109. The Temporary Suspension of Telecom Services (Public Emergency of Public Safety) Rules, 2017, https://dot.gov.in/sites/default/files/Suspension%20Rules.pdf.

Home Department to suspend telecom services where necessary, unavoidable, or during a public emergency.[110]

According to the Software Freedom Law Centre, between 2012-2022, there have been 665 internet shutdowns in India.[111] However, this is a flawed approach towards tackling information disorder. It is expensive, having cost the country billions of dollars,[112] ineffective, and unlikely to actually prevent the dissemination of disinformation.

3. The scope of the Election Commission of India does not extend to foreign interference

The Election Commission of India is a permanent independent constitutional body established under Article 324 of the Constitution of India.[113] The ECI is responsible for preparing electoral rolls and conducting elections at the State and Union levels. It maintains and enforces a Model Code of Conduct to make the entire process free, fair, democratic, and accessible for all its stakeholders. The ECI has also issued instructions with respect to the use of social media in election campaigning. Some of the guidelines include the pre-certification of all political advertisements and the applicability of the Model Code of Conduct on activities on social media platforms as well.[114] However, the Election Commission of India does not have the legal authority or the technical capacity to take action against foreign interference in elections through psychological operations.

4. The efficacy of Indian institutions to combat psychological operations is yet to be determined

110. Clause 2, The Temporary Suspension of Telecom Services (Public Emergency of Public Safety) Rules, 2017.

111. Rishika Singh, *"Explained: The frequency, reasons, and controversy over internet suspensions by the Government"*, Indian Express, (2022), https://indianexpress.com/article/explained/explained-the-frequency-reasons-and-controversy-over-internet-suspensions-by-the-government-8005450/.

112. Gyan Pathak, *"Internet suspension for quelling protests cost India $4.7 billion"*, The Leaflet, (2022), https://theleaflet.in/internet-suspension-for-quelling-protests-cost-india-4-7-billion/#:~:text=It%20mentioned%20as%20per%20Top,840%20hours%20of%20bandwidth%20throttling; Abhishek Chatterjee, *"Internet shutdowns in 2020 costs India $2.8 billion"*, The Hindu, (2021), https://www.thehindu.com/sci-tech/technology/internet-shutdowns-in-2020-costs-india-28-billion/article33501483.ece.

113. Article 324, Constitution of India

114. Election Commission of India, *"Handbook for Media, General Election to the 17th Lok Sabha, 2019"*.

In 2019, the Defence Ministry created an Information Warfare branch in the army to combat misinformation and propaganda on social media.[115] This was in response to the disinformation and propaganda circulating in social media relating to the Indian Air Force airstrike on a terror camp in Balakot. The cyber unit of the army operates under the Information Warfare branch.[116] However, there is not enough information available in order to determine the efficiency of this branch.

B. Network Warfare

1. Legal treatment of data breaches

The Information Technology Act, 2000 has provisions that provide individuals compensation if a body corporate possessing or handling their sensitive personal data is negligent in implementing reasonable security practices and consequently, causes a data breach.[117] Further, the forthcoming Digital Personal Data Protection Bill, 2022 requires companies to notify affected individuals in every instance of a data breach.[118] Further, if a company fails to take reasonable safeguards to prevent a data breach, they may face a penalty up to Rs. 250 crore.[119]

The Information Technology Act, 2000 also punishes cyber terrorism. Cyber terrorism in this context is denying access to any person authorized to access a computer resource, attempting to access a computer resource without authorization, or introducing any computer contaminant with the intent of threatening the security of the country.[120] This Act is applicable to offences committed outside India by any person, irrespective of their nationality.[121]

115. Shaurya Karanbir Gurung, *"Defence Ministry approves information warfare branch for Indian army"*, Economic Times, (2019), https://economictimes.indiatimes.com/news/defence/defence-ministry-approves-information-warfare-branch-for-indian-army/articleshow/68329797.cms?from=mdr

116. Abhishek Bhalla, *"Defence ministry clears information warfare branch for Army to counter fake news"*, India Today, (2019), https://www.indiatoday.in/india/story/defence-ministry-clears-information-warfare-branch-army-counter-fake-news-1473624-2019-03-08.

117. Section 43-A, IT Act, 2000

118. Clause 9(5), The Digital Personal Data Protection Bill, 2022.

119. Schedule 1, The Digital Personal Data Protection Bill, 2022.

120. Section 66-F, IT Act 2000.

121. Section 75, IT Act, 2000

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 prescribes that social media platforms must report cyber security incidents with the Indian Computer Emergency Response Team.[122] In April 2022, the Indian Computer Emergency Response Team (CERT-In) announced mandatory new cybersecurity guidelines for service providers and intermediaries.[123] These guidelines state that all cyber incidents must be reported to CERT-In within 6 hours of noticing such an incident. Some such incidents include the compromise of critical systems/information, the unauthorised access of IT systems/data, intrusion into websites in the form of unauthorised changes such as inserting malicious codes and links, attacks on servers, data breaches, and unauthorised access to social media accounts.

2. *Institutions tackling network warfare*

The Indian Cyber Crime Coordination Centre is an initiative by the Ministry of Home Affairs which aims to prevent the misuse of cyber space to further the cause of extremist groups, and coordinate activities relating to the implementation of India's Mutual Legal Assistance Treaties with other countries.[124] This scheme consists of various entities for threat analytics, cybercrime reporting, investigating, training, and research. For instance, in 2020, the Indian Cyber Crime Coordination Centre sent an exhaustive list of recommendations that requested the Central Government to block several Chinese apps that are likely to pose a threat to data security and privacy rights of citizens. Resultantly, the Ministry of Information and Technology has invoked Section 69A of the Information Technology Act, 2000 as well as its relevant rules, and blocked 59 applications that it considered was prejudicial to the sovereignty and integrity of India.[125]

122. 3(l), Intermediary Guidelines and Digital Media Ethics Code, 2021

123. Ministry of Electronics and Information Technology, *"Directions under sub-section (6) of Section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response, and reporting of cyber incidents for safe and trusted internet"*, No. 20(3)/2022-CERT-Inhttps://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf

124. Ministry of Home Affairs, *"Details about Indian cybercrime coordination centre (I4C) Scheme"*, https://www.mha.gov.in/division_of_mha/cyber-and-information-security-cis-division/Details-about-Indian-Cybercrime-Coordination-Centre-I4C-Scheme

125. Press Information Bureau, *"Government bans 59 mobile apps which are prejudicial to sovereignty and integrity of India, defence of India, security of state and public order"*, https://pib.gov.in/PressReleseDetailm.aspx?PRID=1635206.

C. Intelligence-Based Warfare

1. FDI Policy and National Security

The Foreign Exchange Management Act, 1999 ("FEMA"), its corresponding rules, and India's Foreign Direct Investment Policy governs foreign direct investment in India. According to the Consolidated FDI Policy as per October 2020, there are restrictions placed on certain foreign actors from investing. Foreign investments by individuals or entities of a country that shares a land border in India (Afghanistan, Bangladesh, Bhutan, China, Myanmar, Nepal, and Pakistan) can invest only via the government route.[126] This means that investors must take prior approval from the Government of India and it must be in accordance with the conditions they have stipulated. However, this policy does not have any specific provisions that pertain to national security.

126. Department for Promotion of Industry and Internal Trade, "*Consolidated FDI Policy*", (2020), https://dpiit.gov.in/sites/default/files/FDI-PolicyCircular-2020-29October2020_0.pdf

V. RECOMMENDATIONS

A. Define and penalise foreign interference in democratic processes

India does not have a comprehensive legal framework that can effectively address the various forms of information warfare operations by foreign actors on social media. While there exists the Information Technology Act, 2000 and its corresponding Intermediary Guidelines and Digital Media Ethics Code, 2021 which recommends platforms to ensure that users do not post misinformation or spread content that is likely to threaten the national security of the country, such provisions are not equipped to identify and take action against the involved foreign adversaries.

Legislative approaches to address information warfare must have clear definitions on the scope of these operations, and who foreign adversaries are. India may introduce penal provisions that specifically target foreign interference in democratic processes on social media. Here, foreign interference can refer to interference that is taken by, or on behalf of a foreign principal. The range of activities that interference constitutes of can include: (i) promoting the interests of a political party or a politically significant entity; (ii) seeking to influence the outcome of any election or national referendum; (iii) seeking to influence the outcomes of proceedings in Parliament or any aspect of the legislative process; or (iv) seeking to compromise domestic information systems including those that have a critical impact on national security. Interference must be in the form of a coordinated campaign on social media which may utilise the creation of bots and multiple false identities. It is important to introduce exemptions for good faith journalism, and legitimate critique of the government so that such provisions do not cause a chilling effect on free speech. Therefore, instances of unintentional or good faith dissemination of content that constitutes foreign interference by individuals must be exempt from penal action, irrespective of the degree of harm.

B. Social media platforms may collaborate with the Election Commission of India to combat psychological operations

Prior to the 2019 elections, representatives of platforms such as Facebook, Twitter, and Sharechat approached the Election Commission of India with

a Voluntary Code of Ethics for the 2019 General Elections.[127] Platforms committed to process violations under Section 126 of the Representation of People Act, 1951 within three hours instead of thirty-six hours. The Voluntary Code required platforms to create dedicated teams to serve as a point of contact for the ECI during the elections. Such a collaboration allowed for the exchange of information and swift action on take down requests. Resultantly, various social media platforms took down content in over 900 instances.[128] The platforms also committed to facilitating transparency in paid political advertisements.[129]

In subsequent elections, platforms must also commit to taking swift action against campaigns by foreign adversaries to interfere in elections. They must be vigilant of activities by coordinated networks of bots and multiple false presences that create and disseminate political content.

C. Law enforcement agencies must collaborate with social media platforms to respond to information warfare

Social media platforms that operate in India must collaborate with law enforcement and the military in order to strengthen the nation's defence against psychological operations. Such a collaboration would involve the regular sharing of analytics data, threats identified, and potential crisis action plans in order to respond to psychological operations by foreign adversaries. For instance, the Indian Cyber Crime Coordination Centre consists of a National Cybercrime Threat Analytics Unit, the objective of which is to create a multi-stakeholder environment and produce cybercrime threat intelligence reports.[130] To that end, domestic social media platforms can establish a jointly managed database of video and image hashes that

127. Press Information Bureau, *"Social Media Platforms present "Voluntary Code of Ethics for the 2019 general election" to Election Commission of India"*, (2019), https://pib.gov.in/newsite/PrintRelease.aspx?relid=189494

128. PTI, *"Over 900 Posts Taken Down From Social Media Platforms During 2019 Polls"*, NDTV, (2019), https://www.ndtv.com/india-news/lok-sabha-election-2019-over-900-posts-taken-down-from-social-media-platforms-during-national-polls-2039866

129. Internet and Mobile Association of India, *"Voluntary Code of Ethics for the General Elections 2019"*, https://static.pib.gov.in/WriteReadData/userfiles/Voluntary%20Code%20of%20Ethics%20for%20the%20G.E.%202019.pdf

130. Ministry of Home Affairs, *"Details about Indian Cybercrime Coordination Centre (I4C) Scheme"*, https://www.mha.gov.in/division_of_mha/cyber-and-information-security-cis-division/Details-about-Indian-Cybercrime-Coordination-Centre-I4C-Scheme.

have been flagged as terrorist content. This in turn can be installed into automatic algorithmic detectors that could immediately identify and remove such content, as well as take action against the originators of that content. This multi-stakeholder environment must include social media platforms. Much like the Joint Cyber Defense Collaborative, there must be information fusion in the form of regular analytic and data exchanges to facilitate each stakeholder to take risk-informed coordinated actions. [131]

D. Establish an inter-agency/ministerial committee to review the national security implications of foreign investments

Introduce an inter-agency/ministerial committee similar to CFIUS to review the national security implications of foreign investments from nations that may have interests that are adversarial to our own. Similar to CFIUS, such a committee would require coordination between the Department for Promotion of Industry and Internal Trade, and the Directorate General of Foreign Trade. In the context of investment in social media firms, the Committee may, among other things, use the following points as guidance[132] in reviewing transactions:

1. Implications of foreign investments on domestic capacity to meet national security requirements, including those that fall beyond the purview of the defence industrial base.

2. Effect of a foreign investment transaction on supply chain resilience and security in key technology sectors that include microelectronics, AI, and other critical technologies.

3. Incremental investments that may result in the cessation of ownership or control in a sector or technology to a foreign adversary.

4. Assessing whether a foreign investment transaction provides a foreign adversary, either directly or indirectly, access to capabilities or information databases which could be used/compromised for cyber-attacks.

131. Joint Cyber Defense Collaborative, *"Changing the Cybersecurity Paradigm: A unified cyber defense"*, (2022), https://www.cisa.gov/sites/default/files/publications/JCDC_Fact_Sheet_508C.pdf

132. Summarised from Executive Order 14083, *"Ensuring Robust Consideration of Evolving National Security Risks by the Committee on Foreign Investment in the United States,"* https://public-inspection.federalregister.gov/2022-20450.pdf

5. Assessing whether a foreign investment transaction in Indian businesses that have access to sensitive personal data of Indian citizens involves a foreign adversary.

Such a process should be mindful of ensuring that it does not disrupt the flow of foreign investment or create a chilling effect that has adverse outcomes on Indian start-ups and businesses.

E. Facilitating law enforcement access to data by entering into an Executive Agreement under the US CLOUD Act

A prerequisite to any legal action against foreign adversaries conducting information warfare on social media platforms is the ability of law enforcement to access relevant data from across borders. Some of the most common approaches adopted by countries to access law enforcement related data across borders are Mutual Legal Assistance Treaties, Letters Rogatory, and Direct Data Access Agreements.[133]

1. Mutual Legal Assistance Treaties and Letters Rogatory

The Mutual Legal Assistance Treaty process is a system of bilateral and multilateral agreements by which countries commit to assist each other in criminal investigations.[134] However, the MLAT process has received a lot of criticism. Responses to MLAT requests for information are quite slow, with the United States taking an average of ten months to process the requests it gets.[135] Further, many of the requests are denied or partially satisfied due to the absence of clarity on the rules governing data. Several MLATs were entered into before the information age and may not be adequately equipped

133. Hong Yanqing, *""Game for Laws": Cross-Border Data Access for Law Enforcement Purposes, Models in the United States*, Europe, and China", (2021), https://law.yale.edu/sites/default/files/area/center/china/document/game_of_laws-7.pdf

134. Jonah Force Hill, "Problematic Alternatives: MLAT reform for the digital age", Harvard NSJ, (2015), https://harvardnsj.org/2015/01/problematic-alternatives-mlat-reform-for-the-digital-age/

135. Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies, *"Liberty and Security in a Changing World"*, White House Archives, (2013), https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

to address the complexities of the digital space. India has entered into 42 MLATs of which 18 were entered before 2008.[136]

When there are no MLATs between two countries, they have the option of attempting to seek information through a judicial instrument known as a Letters Rogatory (LR). An LR is a formal request issued by a criminal court seeking the assistance of a court or authority in another jurisdiction.[137] However, this system is arguably even slower than the MLAT route.[138]

In 2019, the Ministry of Home Affairs issued guidelines that clearly define the procedure to send and execute requests for MLATs.[139] These guidelines seek to standardise the applications and ensure that they're not rejected on grounds of not complying with procedural requirements. Further reforms of the MLAT process must be in the form of bilateral or multilateral initiatives where existing MLATs are renegotiated to improve data protection, and transparency.

2. Direct Data Access Agreements

A third, more efficient alternative that countries are beginning to adopt is entering into Direct Data Access Agreements. One of the most prominent examples of this is the US Clarifying Lawful Overseas Use of Data (CLOUD) Act. This Act seeks to permit countries to enter into bilateral agreements with the United States to obtain direct access to electronic evidence that is held by a US based global provider.[140] The Act authorises the US executive to enter into international agreements where select foreign governments can receive data directly from the US without any legal restrictions. However,

136. Turkey (1988), Switzerland (1989), Canada (1998), France (1998), United Arab Emirates (1999), Russian Federation (2000), Kazakhstan (2000) Mongolia (2001), Uzbekistan (2001), Tajikistan (2003), Ukraine (2003), Bahrain (2004), Thailand (2004) Kuwait (2005), Korea (2005), USA (2005), Belarus (2006), Spain (2007) and Bulgaria (2007).

137. Legal Information Institute, *"22 CFR§ 92.54 - "Letters rogatory" defined"*, https://www.law.cornell.edu/cfr/text/22/92.54

138. Gilman, McLaughlin & Hanrahan, *"How long do letters rogatory take to execute?"*, (2022), https://www.gilmac.com/blog/2022/03/how-long-do-letters-rogatory-take-to-execute/.

139. Ministry of Home Affairs, *"Comprehensive Guidelines for investigation abroad and issue of Letters Rogatory/Mutual Legal Assistance Requests and Service of Summons/Notices/Judicial Documents in respect of Criminal Matters"*, F.No. 25016/52/2019-LC, https://www.mha.gov.in/sites/default/files/ISII_ComprehensiveGuidelines16032020.pdf

140. Frequently Asked Questions, https://www.justice.gov/criminal-oia/page/file/1153466/download.

this authorization is contingent on the requesting country's laws adequately protecting privacy, protecting civil liberties, among other conditions.[141]

Similarly, on the EU front, a proposal to facilitate cross-border access to electronic evidence was presented before the European Commission. This mechanism is composed of two instruments: a regulation and a directive. The regulation would include a European Production Order and a European Preservation order.[142] These orders compel service providers in the European Union to produce electronic evidence or preserve it in the event of a subsequent request for production.[143] The unique characteristic of this proposal is that the order to produce data goes directly from the issuing authority in an EU member state to the service provider in another state without the involvement of the authorities in the executive State. This is to improve the effectiveness and speed of processing requests.

India has not yet pursued an agreement with the US Government under the CLOUD Act. This could be attributed to the fact that some of India's laws are incompatible with the conditions prescribed by the CLOUD Act.[144] However, the primary barrier to any negotiation efforts on part of India is the absence of a comprehensive data protection law. The Digital Personal Data Protection Bill was released for public consultation on 18th November, 2022.[145] This Bill provides that its provisions are applicable outside the territory of India when any activity is connected to the processing of data of individuals within the territory of India.[146] Once the forthcoming Data Protection Bill is passed, India can consider entering into negotiations to pursue an agreement under the CLOUD Act.

141. Stephen P. Mulligan, *"Law Enforcement Access to Overseas Data under the CLOUD Act"*, Congressional Research Service, https://sgp.fas.org/crs/misc/LSB10125.pdf.

142. Eur-Lex, *"Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters"*, (2018), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A225%3AFIN

143. https://eucrim.eu/articles/european-commissions-proposal-cross-border-access-e-evidence/#docx-to-html-fnref5

144. Observer Research Foundation, "India-US Data Sharing for Law Enforcement: Blueprint for Reforms", (2019), https://www.orfonline.org/wp-content/uploads/2019/01/MLAT-Book-_v8_web-1.pdf

145. "The Digital Personal Data Protection Bill, 2022", https://www.meity.gov.in/content/digital-personal-data-protection-bill-2022

146. Section 4 (2), Digital Personal Data Protection Bill, 2022.

B-40 First Floor
Soami Nagar South
New Delhi - 110017
contact@esyacentre.org
www.esyacentre.org