
THE COVERT FORCES BEHIND FOREIGN ELECTORAL INTERFERENCE: AN ANALYSIS OF INTERNATIONAL INCIDENTS AND LEGAL COUNTERMEASURES

Gayathri. Narayanan. N, B.A., LL.B.(Hons.), School of Law, SASTRA Deemed to be University, Thanjavur, Tamil Nadu

ABSTRACT

This research paper explores how the underlying dynamics of foreign interference in domestic elections, conceptualized as the “covert force,” vitiate electoral integrity, particularly in democratic societies. Through a comparative analysis of various political events, this paper examines how state and non-state actors influence an electoral outcome by deploying covert strategies and propaganda. The paper also presents a concise case study on the role of technology and cyberspace in exacerbating electoral polls and opinions through pervasive manipulation and how such events have led the government to adopt countermeasures at legislative and institutional levels to reinforce citizens' trust in democratic institutions. This paper proffers recommendations for the adoption of inter-agency engagement and a whole-of-society approach to address this geopolitical crisis in the absence of a standardized international legal framework.

Keywords: foreign electoral interference, general elections, deep-state theory, funded propaganda, democracy.

INTRODUCTION

Every democracy that leads to the formation of a government requires the conduct of free and fair elections to ensure the legitimacy of that government. Electoral integrity plays an intricate role in the functioning of a state. This is often ensured by independent electoral management bodies established as constitutional machinery, like the Election Commission of India¹ or through enactment like the Electoral Commission of the United Kingdom.² Any distortion in the integrity of elections directly results in a threat to democracy. Though much election interference was taking place clandestinely, it became a matter of critical concern worldwide following Russia's interference in the 2016 US Presidential election. This alarmed many countries to assess the integrity of the elections to safeguard the electoral process and the whole concept of state sovereignty in itself. Detecting foreign interference in the election became a primary challenge as it switched to covert methods. This effort is made either to boost the chances of the candidate whose victory may benefit the interferer or to support the campaigns of the candidates whose engagement results in vote splitting. Many researchers began to assess it from an international law perspective as well to determine how far it is considered a breach of state responsibility of non-interference.³ This article is an attempt to analyze the issue of foreign interference in domestic elections and to understand the global approaches taken so far to address this issue. The first part of the article briefly focuses on defining foreign interference in elections by analyzing multiple dimensions adopted to study it globally. The second part classifies what are the major methods of foreign interference by enlisting verified and corroborated incidents through official state documents and election journals. Finally, the article concludes by analyzing approaches adopted by global nations as countermeasures in terms of preventive or proactive measures against election interference.

FOREIGN INTERFERENCE IN ELECTION

Foreign interference in elections occurs when one nation acts to intervene in the electoral process or proceedings of another nation. The interference is often made with a vested interest to disrupt or influence the electoral outcomes by polarizing public opinions and manipulating

¹ Election Commission of India, About ECI, Election Commission of India, <https://www.eci.gov.in/about-eci> (last visited Feb. 16, 2025).

² Political Parties, Elections and Referendums Act 2000, [legislation.gov.uk, https://www.legislation.gov.uk/ukpga/2000/41/contents](https://www.legislation.gov.uk/ukpga/2000/41/contents) (last visited Feb. 16, 2025).

³ U.N. Charter art. 2, ¶ 7

the voters' behavior. The globalized economy has transformed the general elections that happen within a country into a matter of concern for foreign states, international actors, and agencies, as it will have an impact on the foreign policy of that country vis-a-vis the geostrategic interests of others. Foreign interference is regarded as illegal as the interference ultimately leads to the political instability of a sovereign country in which the people have the freedom of opinion and expression to express their political will freely. This cognitive effect has the potential to disrupt the confidence of the people in the democracy itself. In a study conducted by Jonathan Davies, titled "Foreign Election Interference and Hybrid Warfare," election interference is regarded as hybrid warfare, where the "hybridized interference is likely to adopt both candidate and process interventions, but these will be geared towards the erosion of political institutions and societal cohesion"⁴. Julia Brooks, in her article "Election Interference Under International Law," opined that though election interference is an infraction against a nation's political independence, definitional ambiguity on the term 'use of force' in international law impedes considering it as cyberwarfare. Moreover, the statement of Former Central Intelligence Agency Director Michael Hayden cautioned against the use of the term warfare against Russian interference in the US elections.⁵ Steven Wheatley's work which focused on analyzing the non-intervention principle from the lens of the 1986 Nicaragua case concluded that foreign cyber operations that are organized to disable the electoral functioning of another country is a form of coercion⁶ violate the non-intervention principles and therefore breaches the international law, even though the case left the interpretation of the term 'coercion undefined. Hence, it can be understood that though election interference is clearly violative of the non-intervention principle of international law there is a lack of consensus and legal obscurity to consider the same as warfare.

METHODS OF FOREIGN INTERFERENCE

This section of the article deals with the major methods of foreign electoral interference. The interference of a foreign state in another's domestic affairs need not always be direct. An example of an open threat to the electorate or political class is the one made by US President

⁴ Jonathan Davies, *Foreign Election Interference and Hybrid Warfare* (2021) (Senior Indep. Study Thesis, College of Wooster), <https://openworks.wooster.edu/independentstudy/9443>

⁵ Julia Brooks, *Election Interference Under International Law*, Int'l L. & Pol. Online Forum, Winter 2020, at 1, <https://www.nyujilp.org/wp-content/uploads/2020/05/Brooks-Annotation.pdf>.

⁶ Steven Wheatley, *Foreign Interference in Elections Under the Non-Intervention Principle: We Need to Talk About "Coercion"*, 31 Duke J. Comp. & Int'l L. 119 (2021), <https://scholarship.law.duke.edu/djcil/vol31/iss1/3/>.

Donald Trump using his Twitter (now known as X) account in which he warned Iran of “consequences the likes of which few throughout history have ever suffered” if the Iranian leadership continued to threaten the United States”.⁷ At the same time, an example of such an implied threat is the 2007 distributed denial of service (DDoS) attack by Russia on the websites of the Estonian President, Prime Minister, and Parliament, causing an extensive disruption to the political order of the country.⁸ The condemned act of Russian interference in the 2016 US Presidential elections is significant to understanding the degree of illegality and consequences. The US officially acknowledged foreign interference in its sovereign affairs, regardless of the potential political turmoil that may result from the same. The Report On The Investigation Into Russian Interference In The 2016 Presidential Election, also called the Mueller Report⁹ detailed how Russia principally carried out the operation, which included social media campaigning favoring Donald J Trump and disparaging Hillary Clinton. Another method was “computer intrusion operations against agencies and members involved in the campaign of Hillary Clinton and releasing stolen documents.”¹⁰

Election interference takes a myriad of forms. For the convenience of the study, the paper has categorized types of foreign election interference into 4 major heads and provides a case study of electoral interference incidents to each head for the analysis.

1. DISINFORMATION

Disinformation is one of the widely adopted tactics of foreign election interference. It often operates with propaganda to disseminate false, deceiving, and manipulative information among the people to polarize or influence their choices and behavior in elections. Disinformation is misleading and is disseminated to induce false beliefs¹¹. The purpose of disseminating such information is to amplify untrue political messages. The French government adopted the term “information manipulation” instead of disinformation to highlight the political motive behind information manipulation

⁷ Rick Gladstone, *Trump Threatens Iran on Twitter, Warning of Dire ‘Consequences’*, N.Y. Times (July 22, 2018), <https://www.nytimes.com/2018/07/22/world/middleeast/trump-threatens-iran-twitter.html>.

⁸ Steven Wheatley, *Foreign Interference in Elections Under the Non-Intervention Principle: We Need to Talk About “Coercion”*, 31 Duke J. Comp. & Int’l L. 119 (2021), <https://scholarship.law.duke.edu/djcil/vol31/iss1/3/>.

⁹ Robert S. Mueller III, *Report on the Investigation into Russian Interference in the 2016 Presidential Election*, at 1, U.S. Dep’t of Justice (2019).

¹⁰ Ibid

¹¹ Don Fallis, *What Is Disinformation?*, 63 Libr. Trends 401, 406 (2015).

campaigns as the core attributes of the phenomena¹² The advent of social media has tremendously expedited the dissemination of disinformation over which no government has control unless it is verified by the social media platforms and suspended, as the sharing of any political opinions or information on social media is part of the ‘right to freedom of speech and expression fundamental right’ in democratic countries.

Disinformation Campaigns in the 2016 US Presidential Elections

According to a study conducted by Allon J. Uhlmann and Stephen McCombie, a mixture of formal agencies like FSB, GRU, and SVR ¹³ were involved in the disinformation campaign in the 2016 elections. The Internet Research Agency (IRA), a privately owned St. Petersburg-based company controlled by pro-Putin oligarch Yevgeny Prigozhin, played a significant role in information warfare activities.¹⁴ The Mueller report has highlighted that the IRA, which employed hundreds of people, played a colossal role by operating through various social media, including Facebook, Twitter, YouTube, and Instagram, to disseminate disinformation. Most of its activities involved “fabricating online American personas that could spread disinformation or sow division while appearing to be real Americans.”¹⁵ Thus, it did not promote any coherent narratives but completely blurred the lines between falsehood and reality. The fact that some Russian social media profiles, such as @TEN_GOP, were able to overpower their legitimate counterparts demonstrates the success of IRA disinformation in shaping the opinions of at least some Americans.¹⁶

Indian Lok Sabha Elections 2024

India has the largest electorate in the world, with 96.88 crores registered voters ¹⁷ and

¹² Jean-Baptiste Jeangène Vilmer et al., *Information Manipulation: A Challenge for Our Democracies* (2018), https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf (Policy Planning Staff, French Ministry for Europe and Foreign Affairs).

¹³ Allon J. Uhlmann & Stephen McCombie, *The Russian Gambit and the US Intelligence Community: Russia's Use of Kompromat and Implausible Deniability to Optimize Its 2016 Information Campaign Against the US Presidential Election*, 68 Libr. Trends 558 (Spring 2020), <https://www.ideals.illinois.edu/items/116961>.

¹⁴ Jonathan Davies, *Foreign Election Interference and Hybrid Warfare* (2021) (Senior Indep. Study Thesis, College of Wooster), <https://openworks.wooster.edu/independentstudy/9443>

¹⁵ *Ibid*

¹⁶ *Ibid*

¹⁷ Press Information Bureau, Govt. of India, *Press Release No. 2005189* (Feb. 2024), <https://pib.gov.in/PressReleasePage.aspx?PRID=2005189>.

with 642 million people exercising their franchise, the 2024 Lok Sabha elections in India testify that India is the world's largest democracy. India assumed the mantle at the global level by hosting the 2023 G20 summit and creating a milestone with breakthrough innovations in sectors like technology, healthcare, and agriculture. The 2024 Lok Sabha elections, in which PM Narendra Modi contested for his third consecutive term, became nothing short of a spotlight around the world. Astonishingly, warnings about the potential interference of China misusing AI targeting the 2024 Indian elections were circulated by Microsoft.¹⁸ There is no official statement by the government of India acknowledging the electoral interference of China in India. Nevertheless, according to a project titled Foreign Information Manipulation and Interference (FIMI), published by Doublethink Lab, the research team identified a dataset of incidents that showed how Chinese propaganda tried to undermine Indian democracy. In the article *Watch Our Neighbourhood: Collaborative Approaches to Address FIMI During the India Election*, Medium, it was revealed that, 19 pro-PRC originators initially posted concerning three topics: (1) the India-China border clash; (2) India's heatwaves; (3) the sale of BrahMos missiles to the Philippines on X, formerly Twitter. Subsequently, 91 bot accounts with limited followers retweeted at least two of the three topics.¹⁹ However, the active social media rebuttals of the political parties succeeded in tackling disinformation awareness and overcoming the Chinese propaganda with minimal impact.

2. CYBERATTACKS

A cyberattack is the unethical process of attempting to gain unauthorized access to any information from a computer or network. Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself²⁰. Cyberattacks in the electoral process involve an array of mechanisms like hacking, circulation of deepfakes, AI-generated Bots, etc.

¹⁸ Clint Watts, *China's Use of AI to Influence Global Elections: Insights from the Microsoft Threat Analysis Center*, Microsoft On the Issues (Apr. 4, 2024), <https://blogs.microsoft.com/on-the-issues/2024/04/04/china-ai-influence-elections-mtac-cybersecurity/>.

¹⁹ Doublethink Lab, *Watch Our Neighbourhood: Collaborative Approaches to Address FIMI During the India Election*, Medium (Apr. 2024), <https://medium.com/doublethinklab/watch-our-neighbourhood-collaborative-approaches-to-address-fimi-during-the-india-election-727e3e5f0171>.

²⁰ Nat'l Inst. of Standards & Tech., *Cyber Attack*, NIST Computer Security Resource Center, https://csrc.nist.gov/glossary/term/cyber_attack (last visited Feb. 16, 2025).

Cyberattacks have opened up a myriad array of new vulnerabilities. Artificial intelligence has the potential to tremendously increase the amount of disinformation produced by malicious actors. One of the most concerning recent developments is the use of AI to produce compelling fabricated videos known as “deepfakes”. Such videos are produced by feeding existing images or videos of a target into a deep-learning algorithm. With enough input, these algorithms can create high-quality videos of a target saying or doing almost anything.²¹ The integrity of electoral processes is heavily reliant on the security of digital infrastructure, including voter databases, electronic voting machines, and communication networks²² and any cyberattack over the same disrupts the entire political outcomes in elections.

The 2017 French Presidential Elections

The 2017 National elections in France are an example of a brazen attempt by Russia to meddle in the elections by launching cyberattacks. The hackers stole sensitive information and “diverse documents, such as emails, accounting documents, and contracts”²³ by hacking the *En Marche!* (Let’s Go) the campaign team of Emmanuel Macron. They also carried out a “disinformation campaign that comprised of rumors, disinformation, and forged documents, and leaked 15 gigabytes of stolen data, which included 21,075 emails, two days before the second and final round of the French presidential election, just hours before the media cooling-off period began”²⁴ The ‘Macron Leaks’ which consisted of both real and forged emails that seemed fake created a suspicion on public minds about the authenticity of the information. For eg: “real emails in the hacked cache that could have damaged the Macron campaign, such as one that argued that “it is necessary that we lay off as many employees as we can after May 5,” could not immediately be assumed authentic, so the controversy did not take root.”

²¹ *Supra Davies* <https://openworks.wooster.edu/independentstudy/9443>

²² The Invisible Hand of Foreign Interference in General Elections: Examining Its Impact on Indian Democracy and National Progress, *Chintan – India Foundation* (2024), <https://chintan.indiafoundation.in/articles/the-invisible-hand-of-foreign-interference-in-general-elections-examining-its-impact-on-indian-democracy-and-national-progress/>.

²³ Angelique Chrisafis, *Emmanuel Macron Targeted by Hackers on Eve of French Election*, The Guardian (May 6, 2017), <https://www.theguardian.com/world/2017/may/06/emmanuel-macron-targeted-by-hackers-on-eve-of-french-election>

²⁴ Gyanesh Kudaisya, *Foreign Interference in Domestic Politics: Responses from Singapore*, RSIS Policy Report (Apr. 9, 2020), https://www.rsis.edu.sg/wp-content/uploads/2020/04/PR200409_Foreign-Interference-in-Domestic-Politics.pdf.

²⁵ The French government's preparedness after the US election, with advanced tools to counter cyberattacks and massive public awareness campaigns on the impact of disinformation and foreign interference through cyberattacks, coupled with Macron's campaign team's prompt approach, helped Macron to win the Presidential election by successfully overcoming the interventions.

3. COVERT FUNDINGS

Financial contributions and funding play a decisive role in the election campaigning process in all multiparty democratic countries. The successful campaign programs of every political party are substantially reliant on funding. Essentially, this has become a soft target and is highly susceptible to foreign election interference that threatens electoral integrity. According to the political finance database published by International IDEA,²⁶ which selected around 181 countries as samples to assess the ban and limits on donations from foreign interests to political parties, more than 70 percent of the countries around the world have banned such foreign donations. This restriction is often overcome through covert funding. It takes several forms where the flow of funds may be from single individuals to multinational entities with vested interests in the countries they seek to influence in the elections. "Foreign entities may seek to influence elections by channeling covert funding to political parties, candidates, or affiliated organizations. Such financial support can distort the playing field, providing certain actors with an unfair advantage in terms of campaign resources, advertising, and outreach efforts."²⁷ Covert funding is referred to as "maligned finance" in a police brief report titled 'Covert Foreign Money' authored by Josh Rudolph and Thomas Morley.²⁸ It is defined as the financial contribution made to contesting political parties, electoral

²⁵ Seth G. Jones, *Successfully Countering Russian Electoral Interference*, Ctr. for Strategic & Int'l Stud. (May 21, 2019), <https://www.csis.org/analysis/successfully-countering-russian-electoral-interference>.

²⁶ Int'l Inst. for Democracy & Electoral Assistance (IDEA), *Regulations on Foreign Interference in Elections*, https://www.idea.int/data-tools/data/question?question_id=9194&database_theme=302 (last visited Feb. 16, 2025).

²⁷ The Invisible Hand of Foreign Interference in General Elections: Examining Its Impact on Indian Democracy and National Progress, *Chintan – India Foundation* (2024), <https://chintan.indiafoundation.in/articles/the-invisible-hand-of-foreign-interference-in-general-elections-examining-its-impact-on-indian-democracy-and-national-progress/>.

²⁸ Josh Rudolph, *Covert Foreign Money: Financial Loopholes Exploited by Authoritarians to Fund Political Interference in Democracies*, Alliance for Securing Democracy, German Marshall Fund of the U.S. (Aug. 2020), <https://securingdemocracy.gmfus.org/wp-content/uploads/2020/08/Covert-Foreign-Money-Policy-Brief.pdf>.

candidates, political campaigns, influential political elites, or social groups through opaque structures devised to obfuscate a nation-state and its proxies.

NGOs and non-political organizations in the form of charities, associations, foundations, and other non-profits are handy tools for covert funding, as they are inconspicuous in Western countries because of the nature of the socio-legal system there. For example, “far-right parties in Europe such as Alternative für Germany, the Freedom Party in Austria, and the League in Italy each have non-profit conduits that can channel foreign money into elections. Russia secretly funds non-profits serving as bespoke fronts to execute specific mandates, like a Dutch think tank campaigning against a Ukrainian trade deal with the European Union, a Delaware “adoptions” foundation lobbying against sanctions on Russia, environmental groups opposing U.S. hydraulic fracking, and a Ghanaian nonprofit employing trolls pretending to be African Americans”²⁹

Influences on the Brexit referendum

Several allegations indicate the involvement of Russia in the process of Brexit. However, the extent of such involvement to “successfully” influence the campaign remains unclear. The opinions of the people in the Brexit referendum were alleged to be polarized by the Kremlin-based media houses. “Russian government’s English-language TV station, RT, and news website, Sputnik, have conducted systematically one-sided coverage whose effect has been to magnify the ‘Out’ campaign and marginalize the ‘In’ campaign.”³⁰ RT consistently engaged Eurosceptic political leaders Nigel Farage and Jeremy Corbyn in their discussions to express anti-NATO sentiments.³¹ Apart from these covert activities of funded organizations, various social media operations such as trolls and tweets about Brexit were found to be associated with the “Twitter accounts (X) associated with the Internet Research Agency, a notorious troll factory in St. Petersburg.”³² Hence, it can be possibly concluded that the

²⁹ *Ibid*

³⁰ Peter Pomerantsev, *Putin’s Media Are Pushing Britain for the Brexit*, *The Interpreter* (Feb. 17, 2016), <https://www.interpretermag.com/putins-media-are-pushing-britain-for-the-brexit/>.

³¹ Heidi Tworek, *Russian Election Interference: Europe’s Counter to Fake News and Cyber Attacks*, Carnegie Endowment for Int’l Peace (May 23, 2018), <https://carnegieendowment.org/research/2018/05/russian-election-interference-europes-counter-to-fake-news-and-cyber-attacks?lang=en>.

³² *Ibid*

Brexit referendum had also faced foreign interventions, especially that of Russia, to create anti-EU or anti-NATO ideas in the minds of the people of the United Kingdom.

4. ESPIONAGE

Another form of foreign interference that poses a serious threat to electoral integrity and national security is espionage. Foreign intelligence agencies or media houses operated by foreign nations are used as tools for the purpose where they try to collect sensitive information and coerce political leaders to serve their vested interest or use it as a medium to gather information to propagate disinformation campaigns. This has become even more possible with the online electoral process and the interference taking the form of cyber espionage.

Chinese Espionage Allegations

The European Union has always taken a condemnatory stance against the authoritarian regime and atrocious human rights violations in the PRC (China). A recent report by the Friedrich-Hauser Foundation has confirmed the operation of Chinese espionage in the European Parliament (EP) through right-wing populist politics. On April 23, 2024, K. Guo was arrested on charges of spying against EP for the Chinese security apparatus.³³

Guo was an employee of Maximilian Krah, MEP and EU lead candidate of the AfD. Mr. Krah has also been accused of corruption for receiving money from people linked to Russian leadership. “While AfD politicians such as Krah voted against an EP resolution on foreign interference in democratic processes in the EU, the Liberals in the EP have played a central role in recent years in drawing attention not only to the problem of espionage but also to the danger that can potentially emanate from authoritarian regimes.” And for the same reason, European institutions were vigilant in preventing any distortion in the super-election year 2024.

³³ Liberal Institute, *A Look Behind the Scenes: Chinese Espionage in the European Parliament*, Friedrich Naumann Foundation for Freedom (Feb. 2024), <https://www.freiheit.org/european-union/look-behind-scenes-chinese-espionage-european-parliament>.

DEEP STATE THEORY - a new transnational threat to electoral democracies.

Deep State refers to an alleged secret network of agencies that may consist of unauthorized powerful governmental, non-governmental, corporate elites, or media outlets capable of lobbying the policy decisions of the elected government. This shadowy network goes beyond manipulating the political outcome and extends to as much as manipulating the economic, foreign, and national security objectives.³⁴ The word ‘deep state’ is derived from the Turkish term “*derin devlet*”. “In Türkiye, it refers to a non-elected military elite dominating elected governments, especially when they attempt to dismantle the secular foundations of the Republic, established by Mustafa Kemal Pasha after the abolition of the caliphate in 1923.”³⁵ The term has gained wide attention following the vow of Donald Trump to “dismantle deep state and reclaim our democracy from Washington corruption once and for all,”³⁶ by removing thousands of federal employees from their civil service protections who are responsible for persecuting conservatives without any evidence. He also stated “We will launch a major crackdown on government leakers who collude with the fake news to deliberately weave false narratives and to subvert our government and our democracy,”³⁷

It is referred to as a theory in this section because, despite historical examples, it lacks credible sources or reports to substantiate with evidence and prove that these allegations are true. Nevertheless, the omnipotence of the deep state is vindicated by many other countries making allegations of the same.

The deep-state cabals operate in multiple surreptitious ways which “engineering polls to ensure the election of a sympathetic political party or candidate to the high office via a combination of covert funding, media influence, and disinformation campaigns, topped the list.”³⁸ It is

³⁴ *How the Deep State Uses Censorship and Disinformation to Surreptitiously Further Its Goals*, The Wire (Feb. 2024), <https://m.thewire.in/article/security/how-the-deep-state-uses-censorship-and-disinformation-to-surreptitiously-further-its-goals>.

³⁵ Ravi Joshi, ‘Deep State’ in India — a Convenient Boogeyman for Modern Politics, The Print (Feb. 2024), <https://theprint.in/opinion/deep-state-india-convenient-boogeyman-modern-politics/2477768/>.

³⁶ Eric Katz, *Trump Vows to ‘Shatter’ the Deep State, Revive Schedule F and Move More Agencies Out of D.C., Gov’t Exec.* (Mar. 6, 2023), <https://www.govexec.com/workforce/2023/03/trump-vows-shatter-deep-state-revive-schedule-f-and-move-more-agencies-out-dc/384266/>

³⁷ *Ibid* <https://www.govexec.com/workforce/2023/03/trump-vows-shatter-deep-state-revive-schedule-f-and-move-more-agencies-out-dc/384266/>

³⁸ *How the ‘Deep State’ Uses Censorship and Disinformation to Surreptitiously Further its Goals*, The Wire (Feb. 16, 2025), <https://thewire.in/security/how-the-deep-state-uses-censorship-and-disinformation-to-surreptitiously-further-its-goals>.

shielded from any form of public scrutiny and accountability, conveniently foreclosing any surveillance of its operation.

The allegation of deep state meddling with Indian elections came up during the 2024 Lok Sabha Elections in India as well, where, the BJP leaders accused the Congress party of “using articles by the Organized Crime and Corruption Reporting Project (OCCRP), which is funded by the US Agency for International Development and “other deep state figures” like 92-year-old billionaire George Soros, that “singularly focused” on the Adani Group and its alleged closeness to the government to undermine Modi.”³⁹

Nevertheless, some scholars opine that the deep state conspiracy is used as an excuse by many leaders to deflect criticism against the government. At the same time, “historical examples of its influence in shaping wars, economies, and political regimes lend some credibility to the idea that such shadowy networks do exist and can be both silent in their methods, and deadly in their outcomes.”⁴⁰

GLOBAL APPROACHES

There is no doubt that foreign interference in elections is nothing less than a threat to the democracy of a country. The incidents of such interference around the world have resulted either in cautioning other countries to adopt precautionary or preparatory actions or in warning the targeted nations to intensify the electoral scrutiny by bolstering legislative measures, particularly the cyberspace and the channels of funding. This section of the article analyses and compares the approaches adopted by various countries to tackle foreign electoral interference.

LEGISLATIVE MEASURES

Strong and comprehensive legislation is the first step to combat foreign electoral interference. The prevalence of the law creates awareness in the minds of its people regarding possible foreign subversions in the elections and serves as a form of deterrence against the same.

³⁹ *India: What's behind BJP's 'deep state' charges against US?*, DW (Dec. 17, 2024), <https://www.dw.com/en/india-whats-behind-bjps-deep-state-charges-against-us/a-71083285>.

⁴⁰ *How the 'Deep State' Uses Censorship and Disinformation to Surreptitiously Further its Goals*, The Wire (Feb. 16, 2025), <https://thewire.in/security/how-the-deep-state-uses-censorship-and-disinformation-to-surreptitiously-further-its-goals>.

Singapore is one of the earliest countries to have adopted measures to safeguard electoral integrity and mitigate the risk of electoral interference, both online and offline. The first such enactment is the Political Donations Act of 2001⁴¹. The act was implemented to regulate donations to political parties, political associations, candidates, and election agents in a parliamentary or presidential election to prohibit foreign donations and restrict anonymous donations.⁴² This Act further laid the foundation for the subsequent laws including the Protection from Online Falsehoods and Manipulation Act (POFMA) in May 2019, which was introduced to enhance the transparency of political advertisements and suppress disinformation⁴³ and Foreign Interference (Countermeasures) Act 2021, to prevent, detect and disrupt foreign interference by countering hostile information campaigns (HICs) and through Politically Significant Persons. This Act empowers the Ministry of Home Affairs to impose criminal liability, issue FICA directions, orders such as correctional notices to counter the misinformation, and orders to take down contents, and suspend or disable accounts that engage in spreading hostile information.⁴⁴

The interference of Russia in the 2016 US elections was the crucial incident that led the US to introduce reformative legislative measures. One such measure is the Honest Ads Act⁴⁵ which was incorporated with the For the People Act and was proposed in 2017 and introduced in the Senate in 2023. It expands disclosure rules to regulate online campaign advertisements and increase transparency on critical information concerning the target audience and payment information by requiring social media platforms to maintain a public database of all political advertisements. The Cybersecurity and Infrastructure Security Agency Act, 2018 is another major legislative measure establishing the Cybersecurity and Infrastructure Security Agency. The agency operates as a cyber defense for the federal government and for “coordinating risk assessment and guiding security and resilience across all 16 critical infrastructure sectors (e.g. issuing a directive for federal agencies to secure their cloud environments or publishing

⁴¹ Personal Data Protection Act 2000 (Sing.), https://sso.agc.gov.sg/Act/PDA2000/Historical/20210102?DocDate=20211231&ViewType=Pdf&_=20220422183447

⁴² *Objective of the act* *ibid*

⁴³ Protection from Online Falsehoods and Manipulation Act 2019 (Sing.), <https://sso.agc.gov.sg/Act/POFMA2019>.

⁴⁴ Foreign Interference (Countermeasures) Act (Sing.), <https://www.mha.gov.sg/fica>.

⁴⁵ Honest Ads Act, S.486, 118th Cong. (2023), <https://www.congress.gov/bill/118th-congress/senate-bill/486>.

guidance on protecting infrastructure in the communications sector)”⁴⁶ thereby safeguarding the same from cyber threats and disinformation.

France incorporated their laws to tackle foreign interference in elections in the Electoral Codes, in which legislation regarding the financing of political campaigns is distinguished from financing of political parties. Though political financing has been regulated since 1988, it was only after the 2016 Russian interference that the French decided to fortify their electoral campaign funding. Since January 1, 2018, only French citizens or persons residing in France may make contributions to a political party or group with a threshold set to €7,500 (approximately US\$8,525) per year. Furthermore, to prevent the dissemination of fake news, French law authorizes a judge to order “any proportional and necessary measure” to stop the “deliberate, artificial or automatic and massive” dissemination of fake or misleading information online” during the three months preceding an election.⁴⁷

In India, elections to the two houses of the Parliament and state legislatures are regulated by the Representation of People’s Act, 1951. It prohibits all registered political parties from accepting any contribution from “foreign sources,”⁴⁸ which is defined under the Foreign Contribution (Regulation) Act, 1976. Section 29C of the RPA stipulates requirements and mandates public disclosure of political donations received by political parties and expenditures made for electoral activities.⁴⁹ Laws regarding Disinformation and other cyber operations by domestic or foreign agencies to meddle in the electoral process are governed by the Information and Technology Act 2001 and the institutional machinery of the Election Commission of India. Though India has the RP Act, IT Act, and Manual on the mode Code of Conduct, which is issued by the ECI, to govern the activities of the political parties and the candidates during the election, it lacks a comprehensive law to combat foreign interference.

INSTITUTIONAL MECHANISMS

The pragmatism and effectiveness of a piece of legislation cannot be fully assessed solely based on the potential deterrence it creates, as the functionality of law is sustained and enhanced by

⁴⁶ Cybersecurity and Infrastructure Security Agency, Emerging Tech. Pol’y Careers (Jan. 15, 2025), <https://emergingtechpolicy.org/institutions/executive-branch/cybersecurity-and-infrastructure-security-agency/>.

⁴⁷ Regulation of Foreign Involvement in Elections: France, Libr. of Cong., <https://maint.loc.gov/law/help/elections/foreign-involvement/france.php>.

⁴⁸ Representation of the People Act, § 29B, No. 43 of 1951, India Code (2022), <https://www.indiacode.nic.in>.

⁴⁹ Representation of the People Act, § 29C, No. 43 of 1951, India Code (2022), <https://www.indiacode.nic.in>.

the institutional framework that supports and advances its objectives. Apart from enacting various laws to regulate foreign electoral interference, another major reformative measure adopted by many governments is establishing a robust institutional mechanism to work in tandem. Some of such major initiatives are briefly discussed below.

The US Congress established the Foreign Malign Influence Center (FMIC) in 2019 as one of the five mission centers of the Office of the Director of National Intelligence (ODNI). This mission center aims to “integrate and coordinate the foreign intelligence collection and analysis related to a subject area requiring special emphasis, such as counterterrorism, biosecurity, or—for the FMIC—efforts by foreign malign actors to subvert the U.S. democratic process.”⁵⁰ The Analytical Integration Unit of the FMIC is responsible for providing Indications and Warning (I&W) reports and assessments on foreign adversaries’ capabilities, intentions, and operations to Congress and policymakers by drawing upon the expertise and information from the Intelligence Community (IC). This body also heads the Election Threats Executive and functions as the Intelligence Community’s coordinating authority on election security.

The Federal Government of Australia established the Electoral Integrity Assurance Taskforce in 2018 to ensure public trust in democracy from foreign interference in the electoral processes. The task force consists of various agencies of the government, including the Election Commission, Federal Police, and Security Intelligence Organization. It is responsible for “assessing, understanding, and mitigating these risks and, if required, providing advice to the Electoral Commissioner on how they can best be managed.”⁵¹

India has its own independent constitutional body called the Election Commission of India, established for monitoring, regulating, and conducting all the affairs related to elections. ECI has introduced timely measures to curb any form of interference during elections. ‘Myth vs Reality Register is one such proactive measure adopted to monitor the dissemination of information by debunking fake news regarding elections and verifying the authenticity of the information. “It promotes transparency, accuracy, and responsible communication during elections. It serves as a valuable tool for both the general public and media organizations to access verified information and counter false narratives that may mislead voters.”⁵² The ECI

⁵⁰<https://sgp.fas.org/crs/intel/IF12470.pdf>

⁵¹ Electoral Integrity Assurance Taskforce, Austl. Electoral Comm’n, https://www.aec.gov.au/about_aec/electoral-integrity.htm.

⁵² Myth vs Reality Register, Election Comm’n of India, <https://mythvsreality.eci.gov.in/>.

also ensures access to credible information regarding election people by collaborating with Google⁵³ and Meta⁵⁴.

CONCLUSION

The legislative measures and institutional machinery, coupled with ensuring awareness among people, prove to be an invincible defense against foreign interferences. The Swedish government's effort in response to foreign interference is a lesson that can be adopted by countries around the world to ensure the vigilance and participation of people towards electoral integrity. The Swedes deployed a "whole-of-society approach", which was spearheaded by the government and involved a high-level inter-agency coordination forum⁵⁵, where collaboration with media outlets, students, and international journalists played a crucial role in curbing the dissemination of fake news regarding elections. The French government's approach of 'counter-retaliation for phishing attempt or digital blurring' by placing false flags in confidential and sensitive documents to inundate the hackers is also laudable. However, it cannot function in the long run. A unified international approach to preventing foreign interference in the elections by initiating a platform to share information on the Modus Operandi of the interferer is a preemptive action that is absent at present. While cyberattacks remain a dominant force in election interference, the digital age has empowered all forms of manipulation to infiltrate and operate undetected and wreak havoc through cyber networks. Concomitantly, any countermeasures adopted by the government agencies shall not be at the expense of the democratic rights of its citizens. No country has ever openly endorsed or conceded to interference in the elections of other nations. On the other hand, acknowledging such interference by the aggrieved nations is often viewed as an indication of the vulnerability of their sovereignty. While the power dynamics around the world are constantly shifting, measures to uphold the integrity of the elections to shield democracy shall never be compromised, and for that reason, this subject has to be considered expediently.

⁵³ *Google Ties Up With ECI to Prevent Spread of False Information*, Econ. Times (Mar. 12, 2024), <https://economictimes.indiatimes.com/news/elections/lok-sabha/india/google-ties-up-with-eci-to-prevent-spread-of-false-information/articleshow/108431021.cms>.

⁵⁴ *How Meta Is Preparing for Indian General Elections 2024*, Meta (Apr. 3, 2024), <https://about.fb.com/news/2024/03/how-meta-is-preparing-for-indian-general-elections-2024/>.

⁵⁵ Damien D. Cheong et al., *Foreign Interference in Domestic Politics: A National Security Perspective*, RSIS Pol'y Rep. (Apr. 2020), https://www.rsis.edu.sg/wp-content/uploads/2020/04/PR200409_Foreign-Interference-in-Domestic-Politics.pdf.