Concerns about FIMI: An Indian perspective

November 2023

Funded by
the European Union

DELEGATION OF THE EUROPEAN UNION TO INDIA AND BHUTAN

EU POLICY AND OUTREACH PARTNERSHIP IN INDIA

Concerns about Foreign Information Manipulation and Interference (FIMI): An Indian perspective

November 2023

Authors:

University of Navarra
XKDR Forum

This paper is written in the framework of the EU-India Think Tanks Twinning Initiative 2022-23 — a public diplomacy project aimed at connecting research institutions in Europe and India, funded by the European Union.

Acknowledgements

We thank Anand Venkatanarayanan, Anirudh Burman, Ashish Agarwal, Avinash Godbole, Charmi Mehta, Gauri S Kumar, Harleen Kaur, Manoj Kewalramani, Meghna Bal, Mithila Sarah, Mugdha Mohapatra, Namrata Hasija, Nandkumar Saravade, Nikhil Pahwa, Oleina Bhattacharya, Parushni Jathar, Pratik Datta, Saikat Datta, Shivam Shankar Singh, Shreela Singh, Shubho Roy, Siddarth Raman, Sraboni Roy Choudhury, and Susan Thomas for excellent interviews and discussions.[1]

All errors remain our own.

[1] To facilitate a free flowing discussion we have used, but not attributed, the information we received during our discussions and interviews.

Contents

Acronyms

DIMI Domestic information manipulation and interference.

DOJ Department of Justice.

DPG Digital Public Good.

EEAS European External Action Service.

EU European Union.

FIMI Foreign Information Manipulation and Interference.

HIV Human Immunodeficiency Virus.

IRA Internet Research Agency.

ISC Intelligence and Security Committee of Parliament.

KYC Know Your Customer.

NATO North Atlantic Treaty Organisation.

TTP Tactics, techniques and procedures.

UK United Kingdom.

USA United States of America.

Executive summary

The member states of Global North organisations like the North Atlantic Treaty Organisation (NATO) and the European Union (EU) see the Russian Federation (hereinafter, "Russia") and the People's Republic of China (hereinafter, "China") as primary threats to their security and stability. In this context, a new threat is posed by FIMI, which specifically refers to *non-illegal patterns of behaviour* as opposed to disinformation that covers specific content. While indications of perpetrating FIMI activities can be seen in countries across the world, we focus specifically on Russia and China due to the scale and reach of their operations which have been singled out by NATO and EU member states.

In our report, we offer a uniquely Indian perspective on FIMI. India's uniqueness comes from its sheer size and population, its position as a democracy with relatively free access to the Internet, and also the importance of its large English-speaking population with a sophisticated English-language press. The Indian outlook on Russia and China is very different from those of Global North countries — India saw China as an adversary much before the NATO did, and India does not see Russia as an adversary at all.

Russia and China have different motivations, both for FIMI in general as well as its specific application to India. While Russia seeks to promote discord and distrust among the targeted audience by "confusing, overwhelming and entertaining" the audience, its motivations in India are simpler and are primarily driven by a desire to retain the level of relevance that the Soviet Union once had in India. Specifically, it seeks to present the conflict in Ukraine in favourable terms to promote the strength of its economy, particularly its arms industry, to secure favourable orders.

China, on the other hand, seeks to obtain primacy in the global discourse. It does so by promoting its narrative in favourable terms while engaging in influence operations to strengthen its bargaining position. Regarding India, Chinese objectives for FIMI are twofold: (i) geostrategic primacy, and (ii) competition for influence over other South Asian countries and other countries in the Global South.

When we think of solutions for India, we should address the specific problem of FIMI without opening the door to unintended consequences brought about by low state capacity. This is why we offer solutions that involve research, partnership and cooperation between the government of India, its innovative private sector, research and philanthropic organisations in India as well as in other countries, as well as the global technology giants. This field is ripe for the development of Digital Public Goods (DPGs) and common standards where the EU, its member states, and civil society organisations could certainly play an important role.

1 Introduction

The members of the NATO see the Russian Federation as its "most significant and direct threat" to its security and stability, and the People's Republic of China as a "challenge" to their "interests, security and values" (North Atlantic Treaty Organisation, 2022). The United States, in particular, seeks to "out-compete China and contain Russia" (President of the United States, 2022). In particular, the NATO singles out Russia's "malicious activities in cyberspace" and China's "malicious hybrid and cyber operations" and its "confrontational rhetoric and disinformation" as critical security threats.

These threats are not altogether new — the concept of "disinformation", i.e. "verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public and may cause public harm", is well understood (Colomina et al., 2021). However, the TTPs followed by the "hybrid activities" that NATO refers to have fundamentally changed. Traditional responses to disinformation e.g. appeals to authority based on trust in government have proven ineffective in addressing the large-scale propagation and capture of content on the internet.

Therefore, the European External Action Service (EEAS) in February 2023 defined the term FIMI as "a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes" (European External Action Service, 2023). It further highlighted that FIMI is typically manipulative, intentional and coordinated, and can be conducted by state or non-state actors (including through proxies inside and outside of their own territory) (European External Action Service, 2023; Henin, 2023). This definition diverges from the traditional definition of disinformation which is tied to specific content, while FIMI relates to *patterns of persistent behaviour*.

The EU has taken the lead on detecting, identifying and responding to FIMI in a coordinated manner. The EEAS has set up the Strategic Communication Division (STRAT.2) to monitor disinformation not only among its member states but also in other countries in the region (European External Action Service, 2023). While tackling FIMI, they aim to build capacity among member and other states in order to develop local and coordinated resilience. Individual EU member states have chosen different yet complimentary strategies — for example, France created a dedicated intelligence service like VIGINUM for the purpose of combating FIMI.

While there are many examples of FIMI and other disinformation operations that state actors have allegedly conducted in recent years, this report focuses on Russia and China — the two states that countries in the Global North (e.g. members of the NATO, EU etc.) see as threats due to the scale and reach of their operations.

2 What incentives drive FIMI operations?

Russian motivations for FIMI are largely intended to create discord and distrust in the target audience by "confusing, overwhelming and entertaining" them with a "firehose of propaganda" (Paul & Matthews, 2016). Soviet propaganda, while relying on false narratives when necessary, retained a consistent ideological character. However, today's Russian propaganda is "rapid, continuous, and repetitive" and "lacks commitment to consistency". After all, false news stories are 70% more likely to be retweeted or shared than true news stories (Vosoughi et al., 2018).

Chinese motivations for FIMI are best explained by two separate but related motivational statements. The first motivation for China to engage in influence operations is "discourse power" or the "right to speak" (*huàyǔ quán*) (Friedman, 2022). The concept has many connotations — it conveys Chinese participation and even primacy while setting technical standards (e.g. in artificial intelligence), influence in global media, and market power in the social media sphere (Mattis, 2012).

Retaining primacy over "discourse power" could include the promotion of information and views favourable to China, but it could also include hiding or playing down some negative aspects, such as the targeting of minority ethnic and religious groups, human rights abuses, environmental degradation etc. (Cook, 2020). The second motivation is for China to influence countries in the Global South to appreciate and adopt its own political and economic model (Sukumar & Deo, 2021). Both motivations have informed Chinese disinformation operations, albeit in different ways (Charon & Vilmer, 2021).

3 Relevance of the problem to India

Not only is India the world's most populous country, but also the world's largest democracy. During the Cold War, India was a democratic Non-Aligned nation with a free and vibrant press. These factors offered "an ideal environment to conduct black operations" for both the Capitalist and Communist camps (McGarr, 2021). Even today, India is not part of any large military alliance. India follows a policy of "strategic autonomy" in a manner similar to France during the Cold War — the phrase is originally attributed to Charles de Gaulle (Droin et al., 2023). This is why, while our report focuses on FIMI operations by Russia and China, their motivations for doing so in India are quite different from those of the Global North. Indians see China and not Russia as an adversary.

Today, India is second only to China when it comes to the sheer number of internet users. However, unlike China, internet users in India face fewer restrictions on access. Freedom House's survey on internet freedom places China at the 70th place, Russia at the 65th place, and India at the 40th place among the 70 countries it surveyed (Funk et al., 2023).

India is the world's largest supplier of IT services and IT is India's largest industry (Shah, 2022). This would not have been possible without India's internet freedoms. However, the freedom of entry and expression in Indian cyberspace has also meant that state-sponsored and other actors would find it easier to disseminate information that is detrimental to the core objectives of the Indian state. It is not optimal for India to constrain the freedom of the internet — not only because of India's democratic foundations, but also because doing so would fundamentally threaten the productivity of India's golden goose that is the IT sector (Shah & Suresh, 2023).

India also has the second-largest English-speaking population in the world after the United States. This, along with the presence of a sophisticated English-language press, has meant that India has been the victim of, as well as the source of, English-language disinformation. This has important implications for the English-speaking world as well as those who look to Indian news outlets as credible sources of information.

4 Why is India particularly vulnerable to FIMI?

Broadly, there are four reasons why India is a country that could be particularly vulnerable to the problem of FIMI operations. First, the Indian state faces challenges while making regulations on technology. These largely stem from challenges related to state capacity. The Indian state faces difficulties in defining a technology policy problem that is new and unique e.g. the problem of governing non-personal data, (Bailey et al., 2020), media regulation (Bailey, Shah, et al., 2022) etc. Once the state has understood the problem statement, it faces difficulties in drafting effective regulations e.g. risk-based Know Your Customer (KYC) systems (Parsheera et al., 2021).

Second, once the regulation has come into force, there are state capacity problems when it comes to enforcement (Goyal & Sane, 2021; Parsheera, 2020). This has been seen with issues like surveillance and censorship (Bailey et al., 2018). The state's response to the problem of low capacity often becomes that of giving itself exemptions and special powers, which leads to unintended consequences and does not solve the inherent problem of low state capacity (Bailey & Nair, 2022).

Third, the Indian population has only recently achieved mass-scale literacy. Healthy scepticism of information on social media ideally comes with higher levels of literacy. This has started to take root in India, but it is a steady process (Shah, 2023a, 2023b). Fourth, privacy policies in India are poorly drafted and they fail to explain user rights properly. This leads to a sense of "consent fatigue" where users are not properly aware of their digital rights (Bailey, Parsheera, et al., 2022).

5 TTPs used by Russia and China

At the outset, we note that Russia and China are not the only countries that have conducted FIMI operations. O'Connor et al. (2020) found that between January 2010 and October 2020, 41 elections and 7 referendums were subject to cyber operations, online information operations or both. They trace the source of 38 of these operations to Russia, 10 to China, 4 to Iran and 2 to North Korea. They also note that countries have collaborated on information operations; a finding also shared by the European External Action Service (2023).[2] Figure 1 presents a graphical representation of the TTPs discussed in the following paragraphs.

We also note that there are many examples of FIMI that exist which are unverified in the public domain. Direct accusations of FIMI should ideally be solid enough *"to get a grand jury indictment"* (Cull et al., 2017). We have two broad observations: (i) FIMI may be more visible in advanced economies with high levels of state capacity, and (ii) there is caution about attribution in the public domain. We have interviewed and conducted discussions with a large group of people — most of whom have been thanked in the acknowledgements section. We have shared their insights, in addition to credible academic sources and official reports, while referring to examples of FIMI.

While "information warfare" and smaller-scale cyber attacks have been observed in various countries, it was in 2019 when the USA published the Mueller report that the threat of FIMI firmly established itself in the public sphere (Mueller, 2019). In this report, the USA Department of Justice (DOJ) publicly stated that the Russian government conducted FIMI in relation to the 2016 USA election in a "*sweeping and systematic fashion*" (Mueller, 2019). The interference operation was designed to provoke and amplify political and social discord the USA in 2014-15. Later, a targeted operation was conducted in early 2016 to favour candidate Trump and disparage candidate Clinton. The chief perpetrator of this information operation was Yevgeny Prigozhin and his organisation, the Internet Research Agency (IRA). The operation took two forms: it engaged in targeted advertising and outreach towards minority groups and supporters of candidate Trump on social media, and it also conducted cyber intrusions to release material damaging to the Clinton Campaign (US Department of Homeland Security and Office of the Director of National Intelligence, 2016).

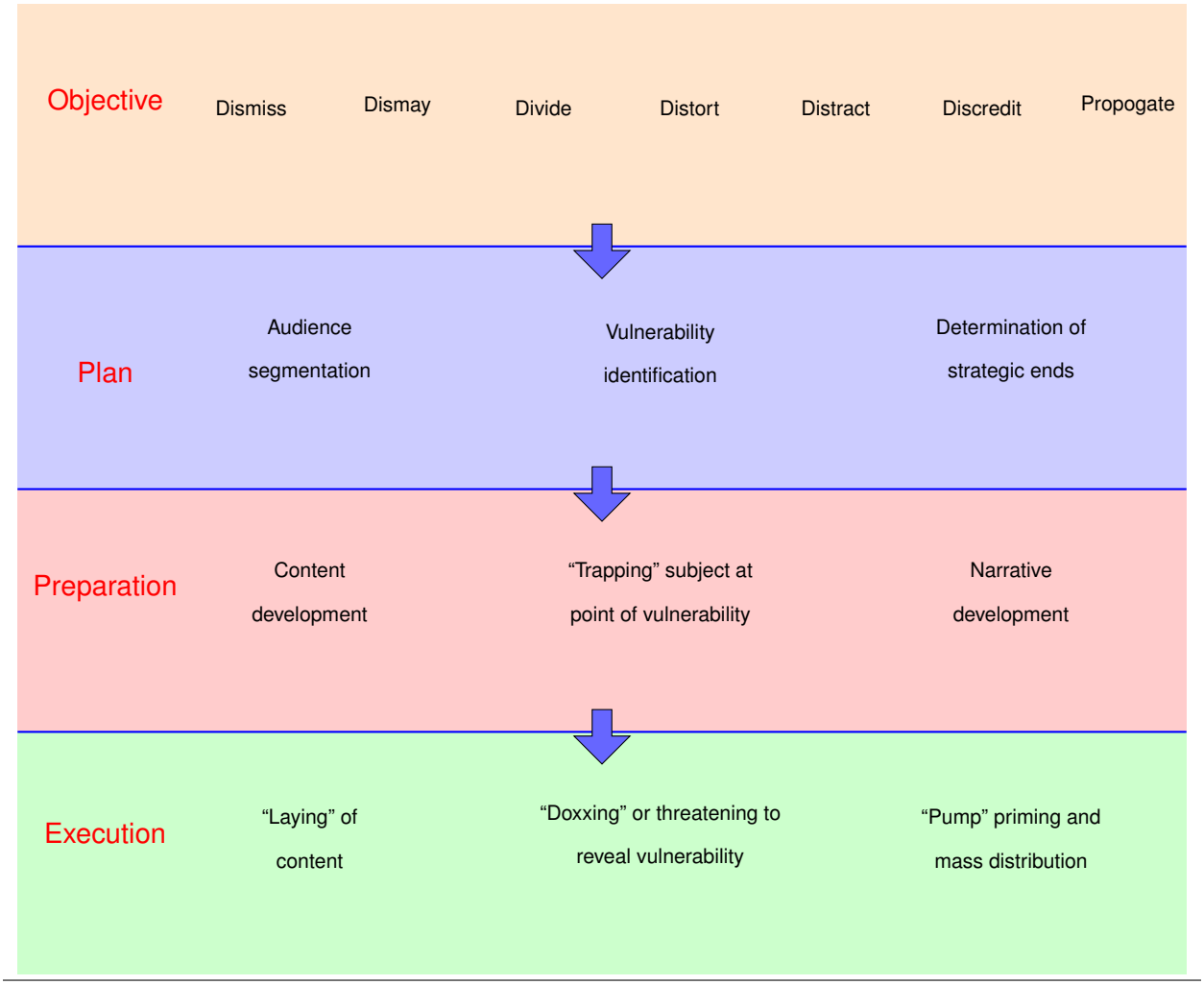
In the United Kingdom (UK), the Intelligence and Security Committee of Parliament (ISC)

[2]We must also note the history of the United States of America (USA) and some of its allies having carried out targeted campaigns to influence elections and the political systems of other countries, especially during the Cold War (Shimer, 2020). However, these actions are not FIMI.

found various examples of disinformation and influence campaigns (United Kingdom Intelligence and Security Committee of Parliament, 2020). For example, Russian state-owned media outlets covered news stories with factual distortions, as well as "hack-and-leak" operations against UK politicians to disrupt the electoral process during the 2014 referendum on Scottish independence.

In Australia, Chinese influence operations have focused on (i) manipulating elite opinion, (ii) buying political access and influence, and (iii) co-opting universities (Searight, 2020).

Figure 1 Offensive framework for FIMI operations. Sources: Newman (2022) and European External Action Service (2023)



6 TTPs specifically used in India by China

In this section, we cover the motivations, techniques, and outcomes of Chinese interference operations that concern India along with some examples. While India-China relations began on a positive note with the *Panchsheel* declaration in 1954, the border conflict of 1962 effectively froze the possibility of deeper relations. The collective memory of the 1962 conflict continues to inform Indian strategic thinking today — it, along with the Chinese nuclear test of 1964, is the direct reason for India's decision to pursue its nuclear weapons program and for India to adopt a "pragmatist" foreign policy (Mukherjee & Sagar, 2018).

China lays claim to the Indian state of Arunachal Pradesh, whilst India considers the Aksai Chin plateau to be a part of the Union Territory of Ladakh. The border question remains unresolved, with recent disputes emerging during the Doklam standoff in 2017 and the violent clashes at Galwan Valley in 2020. After signing their border demarcation agreement in 1963, China and Pakistan have co-operated significantly on issues of military, diplomatic and economic importance, often taking joint positions that are contrary to the Indian position.

The most significant form of engagement between India and China is that of trade. Trade between China and India started to increase following the signing of the Border Peace and Tranquility Agreement in 1993, where both countries agreed to maintain the *status quo* until they reached a final border agreement. Since then, China has become India's largest trading partner. India imports a wide range of goods from China but Chinese imports from India are relatively fewer, leading to a wide trade deficit. India, like its counterparts in the Global North, has sought to reduce its scale of imports from China.

Before we cover some examples of the different types of Chinese information operations, we discuss China's general information strategy, described as "Three Warfares". The first "warfare" is that of influencing public opinion, either by embellishment or by outright manipulation of media and using disinformation. The second is "psychological" in nature, which involves using military, paramilitary, diplomatic, economic and cultural capabilities to intimidate adversaries. Finally, there is "legal warfare", which seeks to use national and international legal regimes to "constrain adversary behaviour, contest disadvantageous circumstances, confuse legal precedent, and maximize advantage" (Quirk, 2021).

We use the categorization provided by the US Department of State (2023) to describe the tools that China is using to reshape the global information environment, namely (i) leveraging propaganda and censorship; (ii) exploiting international organizations and bilateral relationships; and (iii) surveillance and direct actions.

6.1 Leveraging propaganda and censorship

China has made significant investments in expanding the reach and operations of state-owned media in India. Cook et al. (2022) note that Chinese state-owned media outlets have a "notable" influence in India, with Facebook and Youtube pages in Indian languages like Hindi, Bengali, Tamil and Urdu. A report by Freedom House also notes that Indian news agencies have signed syndication agreements where China's main state-run news agency, Xinhua, provides free text and photographic syndication to some Indian news agencies and outlets (Cook, 2020). One person we interviewed informed us that Indian journalists are often invited to programs in China where they are presented with the official narrative of the Chinese position on an issue, which they are expected to write about for their media outlet.

The Communist Party of China has also carried out full-page advertorials in major Indian newspapers (Cook, 2020). While some advertorials cover topics that present Chinese successes on neutral topics (e.g. the 100th anniversary of the Party), others are on contentious topics (e.g. the Chinese position on the South China Sea dispute).[3]

6.2 Exploiting international organizations and bilateral relationships

Chinese officials and diplomats have been known to engage in detrimental coverage of Indian events. The purpose of this is to strengthen China's image for both domestic and international audiences, as well as to undermine Indian influence. There have been important differences in the way Chinese responses in the information space have changed from the Doklam standoff in 2017 to the Galwan Valley clashes in 2020 (Krishnan, 2023). In 2017, public information efforts were to "maintain the absolute superiority of the legal struggle against India" on the "no-smoke battlefield" in the Himalayas. But by 2020, a more coordinated, intense and provocative information campaign was undertaken which was distributed through text and videos on social media.

China has also conducted targeted social media influence campaigns in countries that are neighbours of India. An important example is that of Sri Lanka, where a highly coordinated social media campaign to increase Chinese influence by promoting Chinese culture and China-Sri Lanka relations was conducted on Facebook (Hattotuwa, 2023). Such campaigns were usually not critical towards any country except for a few occasions where China called upon India to join the Belt and Road Initiative (India has refused). Interestingly, the article notes that the Indian High Commission in Sri Lanka has much

[3] India's position is that China should adhere to the arbitral award of 2016 on the South China Sea (Ministry of External Affairs, Government of India, 2023).

lower social media engagement and presence when compared with its Chinese counterparts (Hattotuwa, 2023).

However, we note that attempts at "wolf-warrior" diplomacy have faced backlash, not only in India but even within China. For example, in 2017, a mock conversation between an English-speaking female anchor and a man dressed in a turban and beard and speaking in a mock Indian accent was met with criticism not only in India as well as other countries (Krishnan, 2023). In May 2021, as China celebrated the launch of the "Long March" rocket bound for the International Space Station, India was experiencing the deadly second wave of the COVID-19 pandemic. A senior member of the Central Commission for Political and Legal Affairs shared pictures of the launch alongside a picture of funeral pyres burning at an Indian crematorium, with the caption "China lighting a fire versus India lighting a fire" (CNN, 2021). The post was met with heavy criticism, not only from other users but even from senior Chinese state-media news editors, following which it was taken down. This is perhaps why by 2022 there "appears to be a slow shift away" from aggressive assertions on social media (Hattotuwa, 2023).

6.3 Surveillance and direct actions

Both public and private sector assets in India have suffered cybersecurity breaches and attacks attributable to Chinese actors (Center for Strategic and International Studies, 2023). While direct attacks on public sector assets like the power grid and public sector banks could be considered "cyber warfare", the Chinese attacks on the private sector were targeting news organisations like the Times of India in September 2021 (Center for Strategic and International Studies, 2023). The Times of India operation was intended to gain "early knowledge of media investigations and reporting."

7 TTPs specifically used in India by Russia

In this section, we cover the motivations, techniques, and outcomes of Russian interference operations that concern India along with some examples. Historically, India has not seen Russia as a strategic adversary. On the contrary, during the Cold War, India and the Soviet Union had significant cooperation on three key issues: (i) geo-strategic and diplomatic alignment (e.g. Soviet support for India at the UN) (ii) economic cooperation (e.g. Soviet technical support for India's public sector companies) and (iii) sale of arms (Menon & Rumer, 2022).

After the dissolution of the USSR, India and Russia continued this policy of cooperation. However, the significance of this relationship has reduced. In recent years, India has found new diplomatic and strategic partners (e.g. France, Israel, Japan, and the United States). After India did away with some elements of its command-and-control economy, it enjoyed a period of sustained economic growth. By 2023, the size of the Indian economy will be twice that of Russia. Russia too, has shifted its priorities. Unlike its position during the Cold War, Russia today seeks closer cooperation with China.

Given this background, we observe that the motivations for Russian FIMI operations in India are not the same as those in the Global North. We make a distinction between the Soviet actions during the Cold War and Russian actions after 1991. During the Cold War, Soviet FIMI actions were intended to secure its geo-strategic objectives and to undermine American and British influence in the country. In recent years, while its Soviet-era motivations remain relevant, Russian motivations for FIMI may be informed by its trade relationship with India.

7.1 Understanding the Soviet playbook

To begin with, we must understand the coherent and well-defined set of measures that the Soviet Union developed to conduct information operations in different countries. Soviet propaganda measures consisted of "disinformation" i.e. information that is totally or partially false which advances the Soviet cause. Disinformation would be spread by the KGB using "active measures". Active measures were of three kinds: "white" operations were regular diplomatic, trade and aid operations designed to win hearts and minds, "grey" operations involved the use of foreign Communist parties and media outlets which were not inherently clandestine but the revelation of which may cause embarrassment to the Soviet state, and "black" operations involved genuinely clandestine operations that involve forgeries, blackmail, duping etc. (Kux, 1985)

The Cold War was a conflict of ideologies. Initially, Soviet influence actions were intended to increase support for Communist ideology. However, as the Cold War progressed, Soviet actions increasingly intended to counter the influence of the US and the UK in India. These actions practised a rudimentary form of FIMI and they bear many similarities to the offensive action classification shown in Figure 1.

An example of one such "black" operation was the KGB and the Stasi's efforts to spread disinformation on the Human Immunodeficiency Virus (HIV), codenamed "Operation Denver" (Selvage, 2019a, 2019b). Based on academic sources which rely on declassified East German documents, Table 1 presents the classification of Operation Denver based on the offensive framework for FIMI presented in Figure 1.

Table 1 Example of FIMI: AIDS (Selvage, 2019a, 2019b)

Stage	Description	TTP used
Objective	To "create a favourable opinion of the Soviet Union" abroad by creating a false narrative that HIV was a "bioweapon developed by the United States in secret experiments" that had "escaped the laboratory" and "gone out of control".	Distort, divide, dismay and discredit.
Planning	In July 1983, *Patriot*, an English-language Indian newspaper, published an article titled "AIDS May Invade India: Mystery Disease Caused by US Experiments" which contained false details of "a letter from a well-known American scientist and anthropologist" claiming that the US Department of Defense had developed the HIV "in collaboration with the Center for Disease Control as part of a biological weapons program".	Audience segmentation (the intended audiences were Indians, and members of LGBT communities in English-speaking countries); "laying" and "priming" of content.
Preparation	The KGB's "active measures" program, along with the East German and Bulgarian security agencies, embellished the *Patriot*'s story with more information, both genuine and falsified. For example, the "well-known American scientist" in the *Patriot* article was said to have worked at the genuine establishment that is the US Army Medical Research Institute for Infectious Diseases.	Narrative and content development
Execution	The *Patriot* story, embellished with more information, was published in the Soviet magazine *Literaturnaya gazeta* in October 1985. In December 1985, a British venereologist, John Seale, gave an interview where he claimed that the HIV had been "genetically engineered" by "adding a gene to the visna virus" that affects sheep. Radio Moscow discovered the story and embellished the *Literaturnaya gazeta*'s article with Seale's claims in the following week. In January 1986, leading American immunologist Dr Robert Gallo suggested that the HIV could belong to the same family of viruses as the HTL virus that causes leukemia. While he later withdrew his remarks in the light of new evidence, *Literaturnaya gazeta* in May 1986 used this story to add yet another embellishment to its set of claims as "proof" that the "United States had biologically engineered the HIV" by "using the HTLV as a starter virus".	"Laying" of content through *Patriot*, mass distribution through *Literaturnaya gazeta*, repeated embellishment of the story using a mix of legitimate developments and falsified information to present a coherent narrative, and "pumping" the content on mass media once the story reaches critical traction.

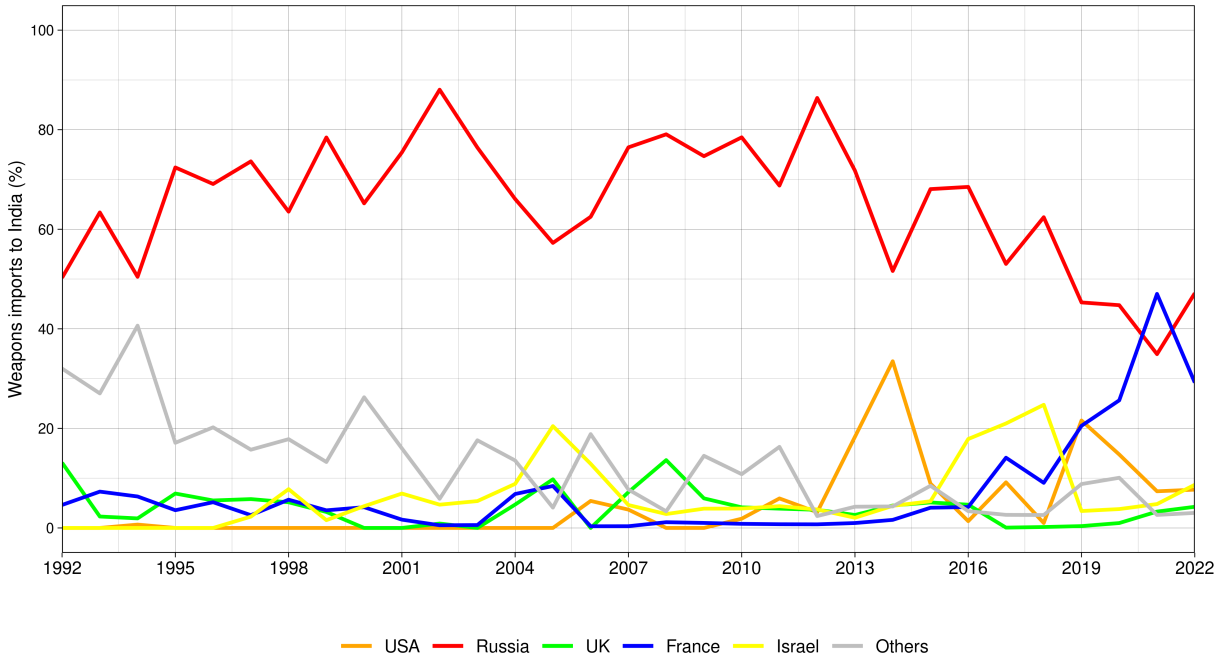
7.2 Information manipulation in the present day

We began by stating that Indo-Soviet cooperation was based on three factors: geostrategic alignment, economic cooperation and the sale of arms. Today, only the third factor is relevant in the Indo-Russian relationship, and this too is declining. Figure 2

shows that, while Russia is still a significant supplier of arms to India, its pre-eminence as such has significantly diminished. By 2021, France had replaced Russia as India's largest supplier by value of arms. India has increased its arms purchases from Israel and the United States. India is also rapidly increasing its domestic production of arms and it has even secured export orders for complex weapons systems like the HAL Tejas fighter aircraft.

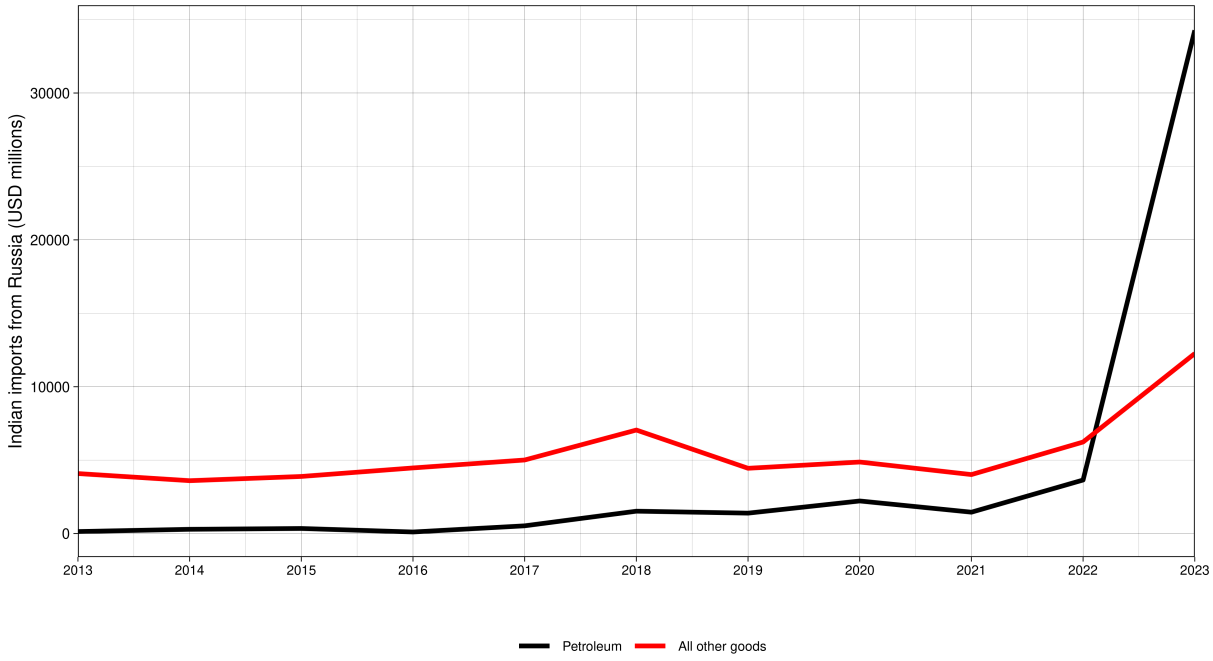
In India, Soviet-era weaponry enjoyed a reputation for being rugged, durable and inexpensive. However, in recent years, Russian weapons have been perceived as inferior in quality compared to their Western counterparts (Bergmann et al., 2023).

Figure 2 Indian imports of arms and weaponry (1992–2022). Source: Stockholm International Peace Research Institute (2023)



The other important element of change in the Indo-Russian trade relationship is India's rapid scale-up of crude oil imports from Russia. Figure 3 shows that India's petroleum imports from Russia increased by seven times in one year (2022–2023). Petroleum constitutes nearly 30% of India's energy mix. 82% of India's petroleum is imported. India's dependence on imports of crude oil is one of its biggest macroeconomic vulnerabilities.

Figure 3 Indian imports from Russia (2013–2023). Source: CMIE Economic Outlook.



7.3 Examples of potential Russian FIMI operations

We now come to the recent developments in Ukraine. It is in Russia's interest to ensure that the Indian audience, especially decision-makers in India, retain confidence in Russian weaponry and Russian oil supplies. Russia may need to project military and economic strength in India to be able to ensure its relevance in the arms export market as well as its crude oil exports to India. Secondary motivations include discrediting and delegitimizing "Western" sources of information. In this context, we share three examples of what could have been Russian FIMI operations.

7.3.1 FIMI operations directly relating to Russian trade interests

In August 2021, Meta released its monthly "Co-ordinated Inauthentic Behaviour" report which mentioned that a UK-registered subsidiary of a Russian marketing firm conducted "a sustained campaign" of misinformation regarding the efficacy of the Pfizer and AstraZeneca vaccines. In November and December 2020, the firm's network posted memes claiming that the AstraZeneca COVID-19 vaccine would "turn people into chimpanzees". In May 2021, the network questioned the safety of the Pfizer vaccine by "posting an allegedly hacked AstraZeneca document". Notably, the network posted much of its content in India in Hindi. The intent behind the campaign was to discredit the two vaccines, one

of which was being produced by an Indian company, and promote the Russian Sputnik vaccine (Medianama, 2021). The campaign was likely begun when the Government of India was considering granting emergency authorization to the AstraZeneca vaccine, which was eventually made available to senior citizens and essential workers in January 2021, and to all adults by May 2021 (Meta, 2021).

The campaign was undone when the Russian firm approached influencers in France and Germany in May 2021. They allegedly offered the influencers a sum of 2000 euros. However, the influencers alerted Meta, which carried out an investigation and took down 65 accounts on Facebook and 247 accounts on Instagram (Meta, 2021).

7.3.2 India as a source for content on Twitter

On 24 February 2022, Russia escalated its conflict in Ukraine. The United Nations General Assembly passed Resolution ES-11/1 on 2 March 2022 which condemned Russia's actions. While 141 countries voted in support of the resolution, India abstained from voting along with 35 other countries. Geissler et al. (2023) studied Twitter activity during the voting at the time of the UN resolution and found that 41.7% of tweets in their sample of nearly 350,000 tweets with a pro-Russian hashtag e.g. `#IStandWithPutin` `#isupportrussia` `#IndiaWithRussia` etc. could be traced to India. These tweets came from nearly 20,000 accounts, 24.2% of which were bots. Similar patterns were observed in countries that had both (i) abstained from voting in the UN resolution, and (ii) a large English-speaking population. These countries, in addition to India, include South Africa, Pakistan and Nigeria. The authors noted that the pro-Russian Twitter accounts in India are engaging with a mostly local audience, suggesting that this is a concerted operation to drive opinion on Twitter in favour of Russia.

At the same time, Geissler et al. (2023) note that India is also a major source of pro-Ukrainian tweets. Among the pro-Ukrainian hashtags e.g. `#DefeatPutin` `#stopputinnow`, they found that 28.57% of these tweets from India were by bots. However, they do not provide the number of pro-Ukraine tweets posted from India.

7.3.3 India as a source of news that serves to "layer" a narrative

The US Department of State (2020) in its report titled "*GEC Special Report: Russia's Pillars of Disinformation and Propaganda*" states that there are English-language websites in India that distribute false narratives that are allegedly promoted by Russian news organisations. Some examples include falsified claims on the shooting down of Malaysian Airlines Flight 17 while flying over eastern Ukraine in July 2014, claims of the US de-

ploying biological weapons against China, etc. We note that, unlike in other countries, the scope and reach of Russian media outlets like Russia Today and Sputnik are very small (less than 30,000 unique visitors per month) (Kling et al., 2022). One person we interviewed informed us that Russia Today has significantly increased its footprint and employee count in India.

8 How India can tackle FIMI: some novel approaches

Given the issues with state capacity in India as discussed in Section 4, we note that a state-led approach with laws and law-enforcement agencies would face certain difficulties.

There is a thin line between FIMI and its domestic counterpart. This is something borne out of the experiences of the Global North countries as well — Russian FIMI in the USA would not have succeeded had it not been for domestic fissures and dissonance in the USA itself. The difficulties of the political system impede enforcement against what might be termed Domestic information manipulation and interference (DIMI). These same constraints will also hamper enforcement against FIMI. These kinds of concerns limit the extent to which a pure state-led path to containing FIMI may induce unintended consequences for society and fare poorly in actually solving the problem.

Against this backdrop, we see the case for an alternative "all-of-society" approach rather than a state-led approach. Our recommendations are directed not just to the EU and the Government of India, but to many other pillars of society. We put forth our recommendations below:

1. Both the EU and the Government of India should deepen their coordination on FIMI. This could be done in three ways:
   (a) The EEAS should increase its engagement with the Indian government agencies on FIMI by opening a route for information sharing. Information sharing would help the Indian security and intelligence agencies to develop further capacity in conducting sharp and non-invasive monitoring of clearly-defined FIMI threats.
   (b) Indian researchers are not directly eligible for research grants under the Horizon Europe research funding program. A dedicated research program should be created where highly skilled researchers from Indian educational institutions and private sector firms alike are invited to offer world-class cybersecurity and policy solutions to combat the problem of FIMI.

(c) The solutions that emerge from these research programs should be in the nature of an open-source Digital Public Good (DPG) which is free to use and replicate.

2. In addition to these state-facing recommendations, we submit the following recommendations for the other pillars of society in both the EU and India:

   (a) It would be wrong to think of the citizenry as completely credulous. There *is* a learning process that always takes place when faced with propaganda and information warfare. Research and policy options need to recognise this popular, cognitive presence of learning and create the conditions to speed up this learning.

   (b) The journalistic profession is built on trust. Globally, we are seeing an increase in subscription-based news services which are of better quality. The journalistic profession, in both India and the EU, should build stronger global and domestic networks of truth-seeking organisations, media organisations, and debunkers of fake news, need to come about through which mainstream information is rendered less vulnerable to information warfare.

   (c) The technology giants need to place a greater priority on their role in impeding information warfare. Shareholders and board members of technology giants need to exert themselves to influence the managers to put a top priority on interfering with information warfare in India including in Indian languages.

   (d) Philanthropists need to see information warfare in general, and FIMI as a major emerging threat to civilised discourse and liberal democracy, and prioritise these "all-of-society" efforts.

9 Prospects for EU-India cooperation

There are important ways in which India can partner with the EU, its institutions and its member states to combat the harmful impact of FIMI on democratic processes. Section 8 discusses some ways of addressing FIMI that can and should be driven entirely with a domestic focus. Yet the space is also ripe for a healthy and fruitful partnership with institutions in the EU and member countries.

We have already mentioned how the EU and India need to improve coordination and joint research funding for the problem of FIMI. This research needs to be in the nature of an open-source framework that helps build a common taxonomy of threats on a global

scale. Efforts like those of the DISARM Foundation, the framework of which has now been adopted across the EU and NATO member states, should be extended to the Indian and global context. This extension is helpful when the EU and its member states share information on threats that they detect. Such frameworks should remain in the nature of a global DPG, where code and resources are freely available on an open-source platform like GitHub. Their use could be promoted by holding training workshops and conferences to create a community of researchers and security analysts from the Global South.

This is where the experience of different EU institutions and member states becomes critical in creating a worldwide community of analysts who can identify, target and mitigate patterns and persistent threats in FIMI operations. Under a well-designed framework, the Indian civil society could directly engage with civil society groups in Europe (such as Correctiva in Germany, Maldita.es in Spain, Pagella Politika in Italy and Demagog in Poland) to collaborate on fact-checking, countering FIMI and disinformation.

References

Bailey, R., & Nair, A. (2022, December 6). *Comments on the draft Telecommunications Bill, 2022* (tech. rep.). Digital Futures Lab. https://www.responsibletech.in/post/comments-on-the-draft-telecom-bill-2022

Bailey, R., Parsheera, S., Bhandari, V., & Rahman, F. (2018, August 6). *Placing surveillance reforms in the data protection debate* (tech. rep.). The Leap Blog. Retrieved November 7, 2023, from https://blog.theleapjournal.org/2018/08/placing-surveillance-reforms-in-data.html

Bailey, R., Parsheera, S., Rahman, F., & Sane, R. (2022). Disclosures in Privacy Policies: Does "Notice and Consent" Work? *Loyola Consumer Law Review*, *33*. Retrieved November 5, 2023, from https://lawecommons.luc.edu/lclr/vol33/iss1/5

Bailey, R., Sane, R., & Parsheera, S. (2020). *Comments on the Report by the Committee of Experts on Non-Personal Data Governance Framework*. SSRN. Retrieved November 7, 2023, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3724184

Bailey, R., Shah, A., Damle, D., & Kaur, H. (2022). *Comments on the Consultation Paper on Issues Relating to Media Ownership*. SSRN. Retrieved November 7, 2023, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4138066

Bergmann, M., Snegovaya, M., Dolbaia, T., & Fenton, N. (2023, September 18). *Seller's remorse: the challenges facing Russia's arms exports*. Center for Strategic and International Studies. Retrieved November 6, 2023, from https://www.csis.org/analysis/sellers-remorse-challenges-facing-russias-arms-exports

Center for Strategic and International Studies. (2023). *Significant cyber incidents*.

Charon, P., & Vilmer, J.-B. J. (2021). *Chinese influence operations: a Machiavellian moment*. Institute for Strategic Research. Ministry of the Armed Forces of France. Retrieved November 6, 2023, from https://www.irsem.fr/report.html

CNN. (2021, May 5). *A Chinese Communist Party-linked account mocked India's Covid crisis on social media. It backfired*. Retrieved November 7, 2023, from https://edition.cnn.com/2021/05/03/china/china-india-weibo-social-media-mic-intl-hnk/index.html

Colomina, C., Sanchez-Margalef, H., & Youngs, R. (2021). *The impact of disinformation on democratic processes and human rights in the world* (PE653.635). European Parliament. Retrieved May 30, 2023, from https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653635/EXPO_STU(2021)653635_EN.pdf

Cook, S. (2020). *Beijing's Global Megaphone: the expansion of Chinese Communist Party media influence since 2017*. Freedom House. Retrieved November 6, 2023, from https://freedomhouse.org/report/special-report/2020/beijings-global-megaphone

Cook, S., Datt, A., Young, E., & Han, B. C. (2022, July 9). *Beijing's global media influence: authoritarian expansion and the power of democratic resilience*. Freedom House. Retrieved

November 7, 2023, from https://freedomhouse.org/sites/default/files/2022-09/BGMI_final_digital_090722.pdf

Cull, N. J., Gatov, V., Pomerantsev, P., Applebaum, A., & Shawcross, A. (2017). *Soviet subversion, disinformation and propaganda: How the West fought against it*. Retrieved May 31, 2023, from https://www.lse.ac.uk/iga/assets/documents/arena/2018/Jigsaw-Soviet-Subversion-Disinformation-and-Propaganda-Final-Report.pdf

Droin, M., Basrur, R., Blarel, N., & Mehra, J. (2023, July 13). *France and India: two nuances of "strategic autonomy"*. Retrieved July 14, 2023, from https://www.csis.org/analysis/france-and-india-two-nuances-strategic-autonomy

European External Action Service. (2023). *1st EEAS Report on Foreign Information Manipulation and Interference Threats: Towards a framework for networked defence*. Retrieved May 31, 2023, from https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf

Friedman, T. (2022). Lexicon: "Discourse Power" or the "Right to Speak" (Huayu Quan). https://digichina.stanford.edu/work/lexicon-discourse-power-or-the-right-to-speak-huayu-quan/

Funk, A., Shahbaz, A., & Vesteinsson, K. (2023, October 15). *Freedom on the Net 2023: the repressive power of artificial intelligence*. Freedom House. Retrieved November 8, 2023, from https://freedomhouse.org/sites/default/files/2023-10/Freedom-on-the-net-2023-Digital-Booklet.pdf

Geissler, D., Bär, D., Pröllochs, N., & Feuerriegel, S. (2023). Russian propaganda on social media during the 2022 invasion of ukraine. *EPJ Data Science*, *12*(1), 35. https://doi.org/10.1140/epjds/s13688-023-00414-5

Goyal, T., & Sane, R. (2021). Towards better enforcement by regulatory agencies. https://datagovernance.org/files/research/1612454004.pdf

Hattotuwa, S. (2023, May 3). Patterns and trends in Chinese propaganda on Facebook in Sri Lanka. In C. Xavier & J. Jacob (Eds.), *How China engages South Asia: Themes, partners and tools*. Center for Social; Economic Progress. Retrieved May 31, 2023, from https://csep.org/wp-content/uploads/2023/05/How-China-Engages-South-Asia-Themes-Partners-and-Tools.pdf

Henin, N. (2023, April 12). *FIMI: towards a European redefinition of foreign interference*. EU DisinfoLab. Retrieved July 6, 2023, from https://www.disinfo.eu/wp-content/uploads/2023/04/20230412_FIMI-FS-FINAL.pdf

Kling, J., Toepfl, F., Thurman, N., & Fletcher, R. (2022). Mapping the website and mobile app audiences of Russia's foreign communication outlets, RT and Sputnik, across 21 countries. *Harvard Kennedy School Misinformation Review*, *3*. Retrieved November 6, 2023, from https://misinforeview.hks.harvard.edu/wp-content/uploads/2022/12/kling_russia_rt_sputnik_audience_20221222.pdf

Krishnan, A. (2023, May 3). New Messengers: The Role of Traditional and New Media in China's External Messaging During India-China Border Crises. In C. Xavier & J. Jacob (Eds.), *How China engages South Asia: Themes, partners and tools*. Center for Social; Economic Progress. Retrieved May 31, 2023, from https://csep.org/wp-content/uploads/2023/05/How-China-Engages-South-Asia-Themes-Partners-and-Tools.pdf

Kux, D. (1985). Soviet active measures and disinformation: Overview and assessment. *US Army War College Quarterly*, *15*(1). https://doi.org/10.55540/0031-1723.1388

Mattis, P. (2012). China's international right to speak. *China Brief*, *12*. Retrieved October 20, 2023, from https://jamestown.org/program/chinas-international-right-to-speak/

McGarr, P. M. (2021). Fake news, forgery, and falsification: Western responses to Soviet disinformation in Cold War India. *The International History Review*, *43*(1), 34–53. https://doi.org/10.1080/07075332.2019.1662471

Medianama. (2021, August 21). *Russian vaccine disinformation campaign about Covishield, Pfizer targetted India: Facebook report*. Retrieved November 6, 2023, from https://www.medianama.com/2021/08/223-vaccine-disinformation-india-facebook

Menon, R., & Rumer, E. (2022). Russia and India: a new chapter. Retrieved November 5, 2023, from https://carnegieendowment.org/2022/09/20/russia-and-india-new-chapter-pub-87958

Meta. (2021, August 9). *Coordinated inauthentic behavior report: July 2021*. Retrieved November 6, 2023, from https://about.fb.com/wp-content/uploads/2021/08/July-2021-CIB-Report.pdf

Ministry of External Affairs, Government of India. (2023, June 29). *Joint statement on the 5th India-Philippines Joint Commission on bilateral cooperation*. Retrieved November 8, 2023, from https://www.mea.gov.in/bilateral-documents.htm?dtl/36743/Joint+Statement+on+the+5th+IndiaPhilippines+Joint+Commission+on+Bilateral+Cooperation

Mueller, R. S. (2019). Report on the investigation into russian interference in the 2016 presidential election. volumes i & ii.(redacted version of 4/18/2019). Retrieved August 8, 2023, from https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1047&context=usjusticematls

Mukherjee, R., & Sagar, R. (2018). Pragmatism in Indian strategic thought: evidence from the nuclear weapons debate of the 1960s. *India Review*, *17*, 12–32. https://doi.org/10.1080/14736489.2018.1415272

Newman, H. (2022). *Foreign information manipulation and interference defence standards: Test for rapid adoption of the common language and framework 'DISARM'*. NATO Strategic Communications Center. Retrieved May 30, 2023, from https://stratcomcoe.org/publications/foreign-information-manipulation-and-interference-defence-standards-test-for-rapid-adoption-of-the-common-language-and-framework-disarm-prepared-in-cooperation-with-hybrid-coe/253

North Atlantic Treaty Organisation. (2022, June 29). *NATO 2022 Strategic Concept*. Retrieved November 8, 2023, from https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf

O'Connor, S., Hanson, F., Currey, E., & Beattie, T. (2020, August 28). *Cyber-enabled foreign interference in elections and referendums*. Australian Strategic Policy Institute. Retrieved July 7, 2023, from https://www.aspi.org.au/report/cyber-enabled-foreign-interference-elections-and-referendums

Parsheera, S. (2020, January 7). *Regulatory governance under the PDP Bill: A powerful ship with an unchecked captain?* https://www.medianama.com/2020/01/223-pdp-bill-2019-data-protection-authority/

Parsheera, S., Sane, R., Verma, R., & Goyal, T. (2021, February 8). *Analysing India's KYC framework: can we do things better?* Indian School of Business. Retrieved November 7, 2023, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3776008

Paul, C., & Matthews, M. (2016). The Russian "Firehose of Falsehood" propaganda model: why it might work and options to counter it. *Perspectives*, (198). Retrieved November 7, 2023, from https://www.rand.org/pubs/perspectives/PE198.html

President of the United States. (2022, October 12). *National security strategy*. Retrieved November 8, 2023, from https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf

Quirk, S. (2021). Lawfare in the Disinformation Age: Chinese Interference in Taiwan's 2020 Elections. *Harvard International Law Journal*, *62*(2). https://journals.law.harvard.edu/ilj/wp-content/uploads/sites/84/HLI205_crop-2.pdf

Searight, A. (2020). Countering china's influence operations: Lessons from australia. *Center for Strategic and International Studies*, *8*, 14.

Selvage, D. (2019a). Operation Denver: The East German Ministry of State Security and the KGB's AIDS Disinformation Campaign, 1985–1986 (Part 1). *Journal of Cold War Studies*, *21*(4), 71–123. https://doi.org/10.1162/jcws_a_00907

Selvage, D. (2019b). Operation Denver: The East German Ministry of State Security and the KGB's AIDS Disinformation Campaign, 1985–1986 (Part 2). *Journal of Cold War Studies*, *23*(3), 4–80. https://doi.org/10.1162/jcws_a_01024

Shah, A. (2022, March 13). *The industry structure of India's large firms: IT is the biggest industry*. Retrieved November 8, 2023, from https://blog.theleapjournal.org/2022/03/the-industry-structure-of-indias-large.html

Shah, A. (2023a, January 23). *Influence operations in India by state actors*. https://www.mayin.org/ajayshah/MEDIA/2023/fimi.html

Shah, A. (2023b, May 15). *Information warfare and its limitations*. https://www.mayin.org/ajayshah/MEDIA/2023/iwar.html

Shah, A., & Suresh, K. (2023, July 18). *The economic cost of small internet shutdowns*. Retrieved November 7, 2023, from https://www.bqprime.com/opinion/the-economic-cost-of-small-internet-shutdowns

Shimer, D. (2020). When the CIA interferes in foreign elections: A modern-day history of american covert action. *Foreign Affairs*.

Stockholm International Peace Research Institute. (2023). SIPRI Arms Transfers Database. Retrieved November 5, 2023, from https://www.sipri.org/databases/armstransfers

Sukumar, A. M., & Deo, A. (2021). The specter of Chinese interference: examining Beijing's inroads into India's digital spaces and political activity. In J. D. Ohlin & D. B. Hollis (Eds.), *Defending democracies*. Oxford University Press. https://doi.org/10.1093/oso/9780197556979.001.0001

United Kingdom Intelligence and Security Committee of Parliament. (2020, July 21). *Report hc 632: Russia*. Retrieved September 18, 2023, from https://isc.independent.gov.uk/wp-content/uploads/2021/03/CCS207_CCS0221966010-001_Russia-Report-v02-Web_Accessible.pdf

US Department of Homeland Security and Office of the Director of National Intelligence. (2016, October 7). *Joint Statement on Election Security* (tech. rep.). Retrieved July 8, 2023, from https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national

US Department of State. (2020). *GEC Special Report: Russia's Pillars of Disinformation and Propaganda*. Retrieved November 6, 2023, from https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%5C%E2%5C%80%5C%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf

US Department of State. (2023, September 28). *How the People's Republic of China Seeks to Reshape the Global Information Environment*. Retrieved November 7, 2023, from https://www.state.gov/gec-special-report-how-the-peoples-republic-of-china-seeks-to-reshape-the-global-information-environment/

Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science*, *359*(6380), 1146–1151. https://www.science.org/doi/abs/10.1126/science.aap9559