DELEGATION OF THE EUROPEAN UNION TO INDIA AND BHUTAN

EU POLICY AND OUTREACH PARTNERSHIP IN INDIA

"Risks, Resilience, Response (3R) – India-EU Cooperation on Russian and Chinese Disinformation and Propaganda"

Funded by the European Union

DELEGATION OF THE EUROPEAN UNION TO INDIA AND BHUTAN

EU POLICY AND OUTREACH PARTNERSHIP IN INDIA

300026954 — PSF-2019-7512

"Risks, Resilience, Response (3R) - India-EU Cooperation on Russian and Chinese Disinformation and Propaganda"

December 2023

Team composition:

The Polish Institute of International Affairs

The Observer Research Foundation

Authors:

Patryk Kugiel

Ankita Dutta

Agnieszka Legucka

Kalpit Mankikar

Filip Bryjka

Sitara Srinivas

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

Table of Contents

Table of Acronyms and Abbreviations

RAS	Rapid Alert System
EEAS	European External Action Service
EoC	European Centre Of Excellence
FIMI	Foreign Information Manipulation And Interference
EU	European Union
IRA	Internet Research Agency
CCP	Chinese Communist Party
DSA	Digital Services Act
TTP	Techniques, Tactics, and Procedures
CSDP	Common Security and Defence Policy
EDMO	European Digital Media Observatory
TTC	Trade and Technology Council
IRI	International Republican Institute
FDI	Foreign Direct Investment

Executive Summary

- India and the European Union (EU), as two of the largest democratic entities, are particularly exposed to foreign manipulation and interference in the information domain. External developments such as Russian aggression against Ukraine in 2014 and border clashes on the India-China border in 2017 have pushed the EU and India to pay more attention to foreign disinformation efforts and invest more in institutional, legal, and educational resilience to counter these challenges. As a consequence, while the EU regards Russia as a major source of disinformation, India focuses exclusively on Chinese activities.
- Despite a growing awareness of a new major threat in the information domain, there is a lack of common understanding between the EU and India about what constitutes “disinformation” and a limited dialogue and cooperation on this issue. This creates space for more EU-India information and intelligence-sharing, exchange of best practices, and discussions about the nature of disinformation and effective countermeasures at both the official and expert levels.
- This research project, implemented in 2023 by the Polish Institute of International Affairs and the Observer Research Foundation and funded by the European Union, aims at an examination and comparison of the approaches of the EU and India to disinformation from two key actors, Russia and China, in order to propose ideas for closer cooperation in this domain. The project team proposes a set of recommendations for the EU and India, including:

    - Launching an **EU-India special dialogue on disinformation** within the EU-India Cyber Dialogue mechanism or the EU-India Trade and Technology Council;.
    - **Inviting India to cooperate with the EU’s Rapid Alert System (RAS**) on disinformation to allow for regular exchange of information on foreign influence operations.
    - **Strengthening the resilience of their respective societies to foreign information manipulation by supporting cooperation and dialogue on disinformation between European and Indian civil society**, experts, academics, and journalists.

- **Engaging in shaping global regulations on disinformation**, also by drawing some lessons from the European Digital Services Act;
- The EU can **establish a new special StratCom unit at the European External Action Service** (EEAS) to better monitor disinformation threats in India and its region;.
- **Supporting the creation of a Centre for Excellence for Countering Disinformation and Hybrid Threats in New Delhi** (like the CoE in Helsinki) or a special **EU-India Disinfo Lab** platform as an academic hub for research and collaboration between Indian and European experts;.
- **Extending the mandate of EUvsDisInfo** to monitor disinformation threats to the EU coming from China; .
- **Supporting the Indian government in developing an official body for monitoring and countering disinformation**, and in raising social awareness and resilience to disinformation;
- **Preparing a public information campaign for the EU and India ahead of the spring 2024 election campaigns** to raise awareness about disinformation and foreign interference in democratic processes and to boost the resilience of European and Indian societies.
- **Supporting further research and analysis on Russian and Chinese disinformation operations in India**

1. Introduction

In an increasingly competitive, unstable, and interconnected international setting, the use of disinformation and propaganda as a tool of foreign policy to influence domestic politics and foreign policy choices in other states has been on the rise. These threats are especially acute in democratic, open, and pluralistic societies like India and European Union Member States. As the **parliaments of both India and the EU are conducting elections in 2024, the risk of foreign interference in this democratic process is an impending challenge;** therefore, engaging this phenomenon to counter it is an urgent necessity for both entities.

Yet, **there is limited experience and literature on EU-India cooperation in this area**. While expansion of the EU-India strategic partnership has attracted attention, there has been no comprehensive comparative study of the European and Indian understanding of the nature and approaches to disinformation threats.

This report is a result of a research project meant to help fill this gap. It was implemented by **two teams of experts, one from Europe (Polish Institute of International Affairs, PISM) and the other from India (Observer Research Foundation, ORF), within the framework of the EU-India Think Tanks Twinning Initiative 2022-2023**. It is based on an extensive literature review on the subject, desk research, and interviews with key stakeholders and practitioners on disinformation in the EU and India. The main findings of the project were discussed and evaluated at a closed-door webinar with experts in November 2023. It helped to refine and sharpen the final conclusions and recommendations. The project focused on disinformation threats in Europe and India from two major external sources: Russia and China. It was designed to address six research questions:

- How is disinformation and propaganda understood in India and the EU?
- What are the EU's experiences with Russian and Chinese disinformation?
- How does the EU deal with and minimise the risks of foreign information manipulation and interference (FIMI) campaigns from Russia and China?
- How serious and well-recognised are Russian and Chinese information interference threats in India?
- What are the strengths and gaps in Indian preparedness and the tools to deal with foreign disinformation?

- Are the current EU-India cooperation mechanisms to counter disinformation sufficient to deal with foreign interference and how can they be improved?

In the following sections, we analyse the phenomenon of disinformation in India and the European Union to identify the gaps and vulnerabilities as well as the preparedness of the Indian and European structures dealing with this challenge. We also look at the prospects of India-EU cooperation in this area and suggest recommendations on how to move forward.

1.1 Note on Terminology

The first methodological challenge of the project was the lack of universally accepted definitions of "disinformation" and "propaganda". As politically sensitive terms, it is not always clear what "disinformation" consists of and who are the main culprits or victims of such activities. What some call "disinformation" or "propaganda" can be "information" and "public diplomacy" for others. This dichotomy is highly relevant to the current study, as there is no mutually agreed definition of "disinformation" in use by the EU and India.

The EU proposes to understand **disinformation** as "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"[1]. However the Union has promoted and used a broader term of **Foreign Information Manipulation and Interference (FIMI)**, which describes "a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures, and political processes. Such activity is **manipulative** in character, conducted in an **intentional** and coordinated manner, by state or non-state actors, including their proxies inside and outside of their own territory"[2].

India, on the other hand, has no official definition of "disinformation". The closest description of it in the Indian legal system is contained in certain provisions of the Indian Penal Code, for example Section 124A, which refers to disinformation used against the workings of the government. Similarly, Section 505 deals with publishing rumours and fear-mongering. In addition, some elements in the Information Technology Act of

[1] European Commission. 2018. "Tackling online disinformation: A European Approach. COM(2018) 236 Final." https://eur-lex.europa. eu/legal-content/EN/TXT/?uri=CELEXper cent3A52018DC0236.

[2] European External Action Service (EEAS). October 2021. "Tackling Disinformation, Foreign Information Manipulation and Interference. Stratcom Activity Report." https://www.eeas.europa.eu/eeas/2021- stratcom-activity-report-strategic-communication-task-forces-andinformation-analysis_en.

2000 refer to false or misleading information. Yet, thus far, no Indian government nor any other non-governmental or expert body has come up with a proposal close to that of FIMI in the EU.

While there are clear definitions that differentiate between misinformation, disinformation, malign information, and propaganda, the conceptual proximity and the frequent use of these terms interchangeably has resulted in a kind of merger of them. The key questions are when does a misinformed opinion become propaganda and how does propaganda take the shape of disinformation? While there are no easy answers to these questions—and these are critical concerns for the countries dealing with the issue—what is clear is that such misused information exploits the vulnerability of the intended audience to push forward a desired narrative in a way that sharpens differences in society and projects public cynicism, uncertainty, distrust, and, in some cases, paranoia.

Therefore, for the purpose of this study, we have used the ***basic understanding of disinformation as the spread of false or manipulated information or a narrative with the intent to influence people.*** It is close to the general understanding of the Indian experts and the EU's FIMI definition in the sense that it underlines the intentional, manipulative, and harmful character of certain kinds of information spread for some other party's benefit.

2. The Disinformation Threat in the European Union – Lessons Learnt

2.1. Risk Assessment

2.1.1 The threat of foreign disinformation in the EU

Over the last decade, there has been a growing recognition of disinformation threats in the Member States of the EU coming from Russia and China. This can be traced back to at least the aftermath of Russia's illegal annexation of Crimea in 2014 when it perpetrated a series of disinformation campaigns and influence operations against Ukraine and Western states. Russian disinformation and propaganda increased in intensity with the outbreak of the war against Ukraine in February 2022. By the end of June 2023, EU institutions had identified more than 16,150 instances of Russian disinformation, as catalogued in the EUvsDisinfo database[3].

While the EU believes that Russian disinformation poses the greatest threat to the Member States because of its systemic nature, in view of Russia's long-term strategy of destabilisation and disintegration of the Euro-Atlantic area, the Union recognises that state as cooperating with other actors, such as Belarus and Iran, as well as with non-state actors[4]. The identification of Chinese disinformation came later, mostly during the COVID-19 pandemic, and it is still not recognised fully across Europe. There is more awareness, including in data, reports, and publications, of Chinese disinformation and influence attempts in Central and Eastern Europe than in Western Europe[5].

During the period from October to December 2022, Russia was responsible for 88% of the recorded information incidents, China for 17%, and—in 5% of cases—there was evident Russian-Chinese cooperation[6]. Notably, 60% of the information manipulation

[3] All information can be found at www.euvsdisinfo.eu.
[4] Russia's national security strategy and military doctrine and their implications for the EU, Directorate-General for External Policies, European Parliament, 2017: Russia's national security strategy and military doctrine and their implications for the EU (europa.eu).
[5] An interview with a European expert on China, Warsaw, 4 September 2023.
[6] European External Action Service, *1st EEAS Report on Foreign Information Manipulation and Interference Threats Towards a framework for networked defence*, Strategic Communications, Task Forces and Information Analysis (STRAT.2), February 2023, [online] https://euvsdisinfo.eu/uploads/2023/02/EEAS-ThreatReport-February2023-02.pdf.

incidents supported Russian armed aggression against Ukraine, while 33% of FIMI attacks directly targeted the Ukrainian authorities.

2.1.2 The message and target of disinformation in Europe

The disinformation strategies employed by Russia and China are primarily centred on propagating the broad assertion that the United States is in a state of decline and is no longer capable of effective global leadership[7]. The focus is on portraying the European Union as subservient to Washington, depicting it as a mere "marionette" or "puppet" controlled by the Americans. The **overarching goal of Russia and China is to create divisions between transatlantic partners** by amplifying anti-NATO and anti-U.S. narratives within European societies. This strategy seeks to undermine the unity and cooperation between EU states and the United States, ultimately weakening the transatlantic alliance. Russia, more so than China, portrays the European Union as a part of a "decaying West" that promotes values conflicting with the conservative way of life in Russian society, particularly with regard to the promotion of LGBTQ+ and sexual minority rights.

More recently, the **main topic of Russia's disinformation relates to Ukraine**. During the Russian-Ukrainian war, a significant focus of the content has been to discredit Ukraine and its society, attempting to weaken their will to fight and reducing international support for Ukraine (both military and humanitarian), and mobilising Russians to go to the front.[8] Russia and China are also responding negatively to the introduction of Western sanctions, which the Russian authorities would like to reduce and/or lift. They try to undermine the legitimacy of the sanctions, portraying them as unjust tools used by Western countries to exert pressure on other states. Also the Western financial system has become a target for both Chinese and Russian disinformation campaigns. As these two countries in particular pursue ambitions for a multipolar world order, they aim to promote alternative financial systems that bypass Western controls and influence[9]. Russia seeks to stoke anti-Ukrainian sentiment in

[7] M. Przychodniak, *Chinese Disinformation: Ideology, Structures, Efficiency,* in: R. Kupiecki, A. Legucka, *Disinformation and the Resilience of Democratic Societies*, PISM, Warsaw 2023, p. 167.
[8] Russia's Strategic and Tactical Narratives in Its War against Ukraine, YouTube: Centre for Democratic Integrity, 28 December 2022., www.youtube.com.
[9] K. Walter, H. Hariharan, *China, Russia Target Western Financial System with Propaganda and Disinformation*, "The Diplomat", 14 July 2023.

order to reduce Western defence and other support and to influence the political debate in Europe.

For China, a very important topic was COVID-19. Its disinformation campaigns sought to distract from the origins of the virus, discredit the United States, and project China as a global leader[10]. Media in Russia copied China's narrative regarding the origins of the virus and argued that the U.S. and other Western democracies "couldn't handle" crises. Russian RT (formerly Russia Today) reported almost daily that social unrest was erupting in Europe due to unnecessary restrictions. By fuelling anti-vaccine narratives and warning against Western vaccines, Russia sought to undermine Europeans' trust in democratic institutions[11].

Russian **FIMI operations in Europe target European societies at large and are designed to distract, divide, and polarise democratic societies**. That is why Russian information campaigns focus on different groups of people and extreme political groups, encompassing both far-left and far-right extremists[12]. The research also shows that **Russia adapts its messages to each specific audience, and therefore it may differ from one country to another**[13]. In Germany, for example, pro-Russian trolls exploit public sentiment about rising inflation and rile up discussions about sanctions, suggesting that they have been more severe for the West than for Russia. In Poland, for example, these trolls use an anti-refugee narrative and harp on about historical disputes between Poles and Ukrainians, aiming to stir up anti-Ukrainian public sentiment and weaken Poles' willingness to help their neighbours[14].

---

[10] J. Kurlantzick, *How China Ramped Up Disinformation Efforts During the Pandemic*, "Council on Foreign Relations", 10 September 2020, https://www.cfr.org/in-brief/how-china-ramped-disinformation-efforts-during-pandemic.

[11] An example of Chinese disinformation involves propagandists creating a fake online persona, for example, "Dr. Wilson Edwards", a user posing as a Swiss biologist on Facebook. This user falsely claimed that the U.S. pressured the World Health Organization to blame China for COVID-19. However, "Dr. Wilson Edwards" was not a real person but a creation of a Chinese cybersecurity company. State-controlled Chinese media still embraced this disinformation, considering the persona an important source on global health policies. For more, see: K. Collier, *China-based Covid disinformation operation pushed fake Swiss scientist, Facebook says*, 1 December 2021, https://www.nbcnews.com/tech/tech-news/china-based-disinformation-operation-pushed-fake-swiss-scientist-faceb-rcna7255.

[12] A. Shekhovtsov, *Russia and the Western Far Right*. *Tango Noir*, Routledge, New York 2018, p. 23-40.

[13] The Kremlin's Trolls Never Sleep, Political Capital, 28 October 2022, www.politicalcapital.hu.

[14] J. Szczudlik, A. Legucka, *Breaking Down Russian and Chinese Disinformation and Propaganda About the War in Ukraine*, „Strategic File PISM", 17 January 2023.

2.1.3 Main actors of disinformation in Europe

Russian and Chinese **disinformation and propaganda campaigns include both state and non-state actors**[15]. Russian FIMI operations are organised by many institutions and, unlike China, they work as a network and in many instances Russian government agencies have been implicated in orchestrating the campaigns[16]. This network involves coordination between the Russian intelligence services (FSB, SVR, GRU), pro-Kremlin media (e.g., RT/Russia Today, Sputnik), the Internet Research Agency (IRA), social media users, diplomatic channels, and academic and cultural institutes.

China's disinformation *modus operandi* is more centralised and employs a multi-tiered approach. It consists usually of primary messages issued by a state actor (e.g., the Chinese Communist Party's [CCP] United Front Work Department in the Central Committee which supervises the disinformation program[17], or statements from the Chinese Ministry of Foreign Affairs), which are disseminated through English versions of party newspapers (like the *Global Times* and *People's Daily*), amplified by accounts on social media, and European "local agents" (can be media companies and newspapers with agreements with the Xinhua news agency). This mechanism includes the Confucius Institutes, cultural and educational centres established by the Chinese government in numerous countries worldwide, including around 190 in Europe alone[18].

2.1.4 Main methods and techniques of disinformation

Russia employs various tactics in its disinformation activities, utilising internet platforms, conventional media, agents of influence, and unwitting individuals, often

---

[15] *European Parliament resolution of 9 March 2022 on foreign interference in all democratic processes in the European Union, including disinformation*, 9 March 2022, https://www.europarl.europa.eu/doceo/document/TA-9-2022-0064_EN.html.

[16] J. Thompson, T. Graham, *Russian Government Accounts Are Using a Twitter Loophole to Spread Disinformation*, "The Conversation", 15 March 2022, http://theconversation.com/russian-government-accounts-are-using-a-twitter-loophole-to-spread-disinformation-178001.

[17] A. Legucka, M. Przychodniak, *Disinformation from China and Russia during the COVID-19 Pandemic*, "PISM Bulletin", 21 April 2020, https://pism.pl/publications/Disinformation_from_China_and_Russia__during_the_COVID19_Pandemic.

[18] Belgium closed the Confucius Institute in that state in 2019, Sweden and Denmark in 2020, and Norway in 2021. For more, see: Pekka Vanttinen, Finland shuts down Confucius Institute amid censorship, espionage accusations, "Euractive", 21 June 2022, euractiv.com/section/politics/short_news/finland-shuts-down-confucius-institute-amid-censorship-espionage-accusations/.

referred to by detractors as “useful idiots”, to spread their disinformation messages. Within this framework, there are usually “little lies” that involve distortions of facts or present biased interpretations. On the other hand, there are also “big lies” in which entirely fabricated information is disseminated on a massive scale to try to replace reality with a created narrative[19]. After conducting extensive monitoring of Russian disinformation over the course of several years, an EU task force unveiled a comprehensive model detailing the patterns of informational and psychological warfare. These techniques (which include strawman fallacy, whataboutism, attacks on and mockery of opponents, provocations, exhaustion, denial) primarily involve obstructing the open and respectful exchange of differing viewpoints by seeking to dominate debate and enforce a specific narrative. By doing so, trolls in particular aim to undermine genuine public engagement and dialogue. Their ultimate goal is to exert influence over societies by exploiting sensitive issues, stoking emotions, and triggering fears and social anxieties.

While Russia and China share specific similarities in their goals and methods of disinformation, there are significant differences in how they approach their actions[20]. Chinese FIMI operations are more complex and sophisticated. Sometimes it is hard to distinguish between them and public diplomacy. **China has relatively recently adopted a more aggressive pattern of disinformation, following in the footsteps of Russia, but it can be said that the country is still learning this style**. In fact, China takes a more reactive approach and seeks international recognition for its vision. **Instead of using fear as a primary tactic, China focuses on building admiration and recognition for its achievements**. Its disinformation campaigns aim to showcase its accomplishments and promote a positive image of itself on the global stage.

At the same time, “China’s FIMI activities do not only focus on propagating its own message but also on suppressing competing voices or messages that would

[19] A classic example of such behavior is the Kremlin’s disinformation campaign regarding Russia’s war against Ukraine in 2022. Russia attempts to convince both international and internal audiences that its actions are in "self-defense," despite the reality being that Russia initiated an attack and invaded a sovereign state that posed no threat.

[20] T. Chłoń, K. Kozłowski, *Selected Case Studies of Systemic Disinformation: Russia and China*, in: R. Kupiecki, A. Legucka, *Disinformation and the Resilience of Democratic Societies*, PISM, Warsaw 2023, p. 38-39.

undermine China's official narrative"[21]. According to the first EEAS Report on FIMI in February 2023, **Chinese tactics include the dissemination of conspiracy theories by Chinese diplomats, officials, and state-controlled media**[22]. China utilises both its own state-controlled media and economic pressure on other media outlets to influence global media relations while simultaneously restricting the activities of foreign correspondents in China. There is also evidence of **China's widening use of paid social media influencers with undisclosed connections to Chinese state-controlled media or other structures, to counter criticisms of China's human rights issues**. China's government and party-state organisations engage counterparts in Europe at various levels: party-to-party diplomacy, local diplomacy (sister cities, sister countries), friendship group, "civil societies" exchanges, business networks, and "NGO" activities at the UN level[23].Concerns about the export of Chinese censorship policies accompany the global expansion of Chinese online platforms, where users of these platforms, such as WeChat, remain subject to Chinese online censorship even when physically outside China's borders.

China and Russia sometimes collaborate in FIMI activities, with Chinese state-controlled media endorsing pro-Kremlin conspiracy narratives, and disinformation flowing between their online FIMI ecosystems[24]. Both countries are adept at leveraging social media and online platforms to disseminate propaganda and disinformation to foreign audiences. They use these channels to promote their narratives, challenge criticism, and advance their geopolitical interests. By employing sophisticated information-warfare strategies, Russia and China seek to shape public opinion, sow confusion, and create divisions in targeted European societies.

2.2. Resilience To FIMI – the EU's Approach

[21] European External Action Service, *1st EEAS Report on Foreign Information Manipulation and Interference Threats Towards a framework for networked defence*, Strategic Communications, Task Forces and Information Analysis (STRAT.2), February 2023, [online] https://euvsdisinfo.eu/uploads/2023/02/EEAS-ThreatReport-February2023-02.pdf.
[22] Ibidem.
[23] *Image control: How China struggles for discourse power*, "Merics", 27 September 2023, Image control: How China struggles for discourse power | Merics.
[24] *Protokoł czetyrnadcatoro zasiedanija Podkomissii po sotrudniczestwu w obłasti sriedsw massowoj informacyi Rossijsko-Kitajskoj Komissii po gumanitarnomu sotrudniczestwu* , Ministerctwo cyfrowogo razwitija, swiazi i massowych kommunikacyj Rossijskoj Fiedieracyi, 29 July 2021 https://www.documentcloud.org.

In the **Strategic Compass**, adopted by the EU Council on 21 March 2022, the focus is on increasing the resilience of states and societies to foreign information manipulation and interference (FIMI) in political processes, as well as broadening the EU's ability to support the Member States in responding to crises caused by hybrid methods. The **primary aim of the EU response to FIMI is to strengthen resilience**, understood as "the ability not only to withstand and cope with challenges but also to undergo transitions in a sustainable, fair, and democratic manner"[25]. This applies to crisis management of both natural and man-made disasters, which include terrorist attacks or hostile action in the form of FIMI incidents. According to the **Action Plan against Disinformation** endorsed by the European Council in December 2018, the EU approach to countering FIMI attacks has four pillars:

(1) identifying, monitoring, and analysing disinformation, as well as responding directly to FIMI incidents;

(2) building resilience within the EU, as well as in partner countries, through training and cooperation with independent journalists and fact-checking organisations;

(3) sharing information through international cooperation, e.g., through the Rapid Alert System (RAS)[26], in cooperation with like-minded partners (e.g., the United States, the United Kingdom, Canada, Japan), and systemic cooperation with NATO;

(4) disrupting disinformation by imposing sanctions and obstructing disinformation perpetrators from attacking[27].

The European Union's ability to respond to disinformation and the character of it is conditioned and limited by the EU's unique status. Issues pertaining to national security and social cohesion are within the competences of the Member States. Thus, **the EU concentrates on them at the supranational level and strives to improve information exchange, develop pan-European institutions, and better coordinate and regulate policies in the information domain**. It is important to remember that specific preparedness to these threats may differ from one Member State to another, yet the EU has designed its own toolbox for the Community level. Specific EU action can be analysed in four dimensions—institutional measures, legal action, educational

[25] *How the EU responds to crises and builds resilience*, European Council, 28 October 2023, www.consilium.europa.eu.

[26] The Rapid Alert System on Disinformation was established in March 2019. Its aim is to increase situational awareness of hostile information manipulation. The exchange of information under this system takes place through contact points set up in individual EU countries.

[27] F. Bryjka, *Tracing the Development of EU Capabilities to Counter Hybrid Threats*, „PISM Strategic File", No. 9, 1 August 2022, www.pism.pl.

initiatives, and international cooperation.

2.2.1 Legal instruments

At the legal level, the EU has undertaken steps to ban certain actors from the information domain in the EU and further improve control over the content of news in the digital world. With the Russian invasion of Ukraine in February 2022, Russian media were finally recognised as tools of information warfare. **In March 2022, the European Council imposed sanctions on the Russian state station RT/Russia Today and the Sputnik** news agency (including their various language versions)[28]. In total, more than 50 propagandists from the Kremlin and other actors involved in Russian disinformation activities were put on the individual sanctions list[29]. However, the Council's decision is temporary. The ban was imposed "until the aggression against Ukraine ceases and the Russian Federation and its associated media cease their disinformation and manipulative activities against the EU and its Member States"[30].

Moreover, individual Member States have taken independent measures (based on national law) to limit the impact of FIMI operations. However, national efforts to curb disinformation depend on the will and determination of the government to actually counter it. The most strict regulations were enacted by Poland, Lithuania, Latvia, and Estonia, but most countries limited themselves to EU-level sanctions. Nevertheless, disinformation actors are able to circumvent these restrictions by using new servers and proxies that enable them to spread false and manipulated content.

In addition to sanctions, the Union has been working for years on systemic legal solutions to curb falsehoods and manipulation on the internet. In **September 2018, the Union adopted the "Code of Practice"** governing EU countries' cooperation with the

[28] Russia Today and subsidiaries, including Russia Today English, Russia Today UK, Russia Today Germany, RT Balkans, Russia Today France, Russia Today Spanish, RT Arabic; Sputnik and subsidiaries, including Sputnik Arabic. In June 2023, Oriental Review, Tsargrad, New Eastern Outlook and Katehon were further restricted as part of the 11th sanctions package.

[29] Among those listed are Rossiya RTR/RTR Planeta, Rossiya 24/Russia 24, Rossiya 1, TV Centre International, NTW/NTV Mir, REN TW, Pervyj Kanal and the media organization RIA FAN, with more being added in subsequent sanctions packages. Restrictions imposed by the EU prevent them from broadcasting material via cable and satellite, as well as broadcasting via internet television, platforms, portals and apps that undermine the democratic order in European countries and aim to polarise EU societies. For more, see: *Council Regulation (EU) No 269/2014 of 17 March 2014 concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine*, 17 March 2014, www.eur-lex.europa.eu.

[30] *EU imposes sanctions on state-owned outlets RT/Russia Today and Sputnik's broadcasting in the EU*, Council of the EU Press release, 2 March 2022, www.consilium.europa.eu.

private sector (including major online platforms such as Facebook, Google, Twitter, Mozilla, and Microsoft) on obligations for online platforms and the advertising industry to improve the transparency of political advertising, close fake accounts, and reduce incentives to spread disinformation. In **2022, the Code was updated** and was signed by 34 private entities. The Strengthened Code of Practice on Disinformation brings together a more diverse range of stakeholders than ever, empowering them to contribute to wide-ranging improvements by signing up to precise commitments relevant to their field. Such commitments include demonetising the dissemination of disinformation, guaranteeing the transparency of political advertising, enhancing cooperation with fact-checkers, and facilitating researchers' access to data[31].

A breakthrough in the fight against disinformation is the **Digital Services Act (DSA),** which was adopted by EU institutions in 2022 and is expected to enter into force on 1 January 2024. Once implemented, the DSA will be the world's first regulation ordering the removal of illegal online content, increasing transparency in the operation of websites, and improving the security of online users. The Act applies to all digital service providers, although the most important provisions are intended for large platforms and search engines. At the same time, the EU hopes that the DSA will become a model for similar legislation in other parts of the world[32].

2.2.2 Institutional measures

Russia's illegal annexation of Crimea in 2014 and disinformation campaign in the Member States compelled EU institutions to build up special mechanisms and tools to better detect and defer FIMI operations. In March 2015, the European Council asked the High Representative for Foreign Affairs and Security Policy to develop an action plan for strategic communications to counter Russia's disinformation campaigns. As a result, a task force responsible for monitoring, analysing, and responding to Russian propaganda and disinformation, **East StratCom, was established within the European External Action Service (EEAS)**. In 2017, two further StratCom task force units were created: one for the Southern Neighbourhood (South StratCom Task Force) and one for the Western Balkans (Western Balkans Task Force).

Russia's full-scale invasion of Ukraine intensified the activities of EU institutions in

[31] *Strengthened Code of Practice on Disinformation 2022*, European Commission, 16 June 2022, www.digital-strategy.ec.europa.eu.
[32] M. Makowska, *EU Agrees the Digital Services Act*, "PISM Bulletin", 16 May 2022, www.pism.pl.

countering disinformation. East StratCom has been strengthened financially and in staffing. It now has 13 full-time employees who can outsource research tasks and analyse how Russia adapts its disinformation techniques and methods to changing situations. East StratCom monitors information messages published in more than 20 languages. Therefore, within the EEAS, similar tasks to East StratCom are carried out by analogous teams (six full-time staff each) responsible for the Western Balkans region and the Middle East and North Africa. They focus on counter-radicalisation, combating propaganda from terrorist organisations as well as disinformation from Russia, China, Iran, and Turkey. In addition, there is a Horizontal Threat Team dealing with Chinese disinformation (four staff members), a team supporting EU missions and operations, a team analysing quantitative data on disinformation techniques, tactics, and procedures (TTPs) used by disinformation actors (three analysts), and two political action teams dealing with building resilience. A team responsible for Africa, which is now seen as the main focus of Russian disinformation operations, will soon be established as a result of French advocacy[33].

All these teams are part of the **40 or so-strong Strategic Communications, Task Forces, and Information Analysis Division at the EEAS**, which supports EU institutions with policy planning, strategy, and strategic communication tools. It also provides support (e.g., analysis and instructions to combat disinformation) for EU diplomatic missions, missions and operations of the Common Security and Defence Policy (CSDP). The unit also develops cooperation with partner countries, the G7, NGOs, civil society, and the private sector (e.g., on data acquisition using modern software and technology). The aim of these activities is to build public awareness and strengthen countries' resilience to disinformation in the EU neighbourhood[34]. In addition, individual Member States have their own strategic communication cells to identify and respond to FIMI threats and incidents.

Within the cooperation with NATO, **in 2017 the European Centre of Excellence (Hybrid CoE) was established in Helsinki**. Participation in the Centre's activities is open to all EU and NATO countries, and the number of Participating States has grown

[33] Based on interviews with EEAS staff, conducted on 21 June 2023 in Warsaw. On Africa's vulnerability to Russian propaganda and disinformation, see: J. Czerep, S. Nowacka, *Fertile ground: How Africa and the Arab World found common language with Russia on Ukraine*, "PISM Report", 17 January 2023, www.pism.pl.

[34] *2021 StratCom activity report - Strategic Communication Task Forces and Information Analysis Division*, 24 March 2022, www.eeas.europa.eu.

to include 34 today. **It acts as a think tank, expert and advisory support, and a platform for sharing experience and information on hybrid threats** (including FIMI). The Helsinki centre primarily contributes to the situational awareness of both organisations by providing expertise and training for countering hybrid threats.[35]

2.2.3 Educational measures

In addition to these technical and legal measures there is an understanding that in the long run **the key role in dealing with disinformation will be education and awareness campaigns** that help make individuals and societies more resilient. Research indicates that countries with high media literacy rates (e.g., Finland, Denmark, Estonia, Sweden[36]) are less vulnerable to misinformation, disinformation, and malinformation threats. Media literacy raises ones' consciousness about the implications of being a channel of disinformation and enables information consumers to make informed judgments about the quality of information[37]. To raise the public's awareness of information risks, programmes that teach critical thinking and media literacy on every level of education are crucial[38]. **The ability to separate fact from opinion, truth from lie, and to recognise manipulated or false content is particularly important in these times of so-called post-truth.**

There are various non-governmental sector initiatives that provide training, workshops, and even online courses are instrumental in increasing public resilience to disinformation (e.g., those provided by GLOBSEC or Debunk.org)[39]. One such example launched at the EU level in June 2020 is the **European Digital Media Observatory (EDMO)** with the aim of increasing EU citizens' resilience to disinformation and equipping them with tools for media education. EDMO has eight regional centres bringing together academics, fact-checkers, and journalists to detect disinformation campaigns, organise awareness-raising activities and critical media

[35] For more, see: https://www.hybridcoe.fi/who-what-and-how/.
[36] *Media Literacy Index 2021*, Open Society Institute Sofia, 14 March 2021, www.osis.bg.
[37] T.D., Adjin-Tettey, *Combating fake news, disinformation, and misinformation: Experimental evidence for media literacy education*, Cogent Arts & Humanities (2022), 9: 2037229, DOI:10.1080/23311983.2022.2037229.
[38] For a lesson proposal for secondary school students, see: J. Podemska, P. Podemski, *Protect Yourself Against Disinformation*, [in]: R. Kupiecki, A. Legucka (eds.), Disinformation and the Resilience of Democratic Societies, PISM, Warsaw 2023, pp. 265-285; for a university-level course proposal, see: F. Bryjka, *Detecting and Countering Disinformation - A Proposal for a Syllabus for a University Course*, [in]: ibidem, pp. 209-234. The book is available in open access format at www.pism.pl.
[39] See: *Civic Resilience Course*, www.debunk.org; *Media & Disinformation: a survival guide to your everyday life on the internet*, www.knowhoax.org.

literacy, and support national authorities in monitoring the practices of online platforms.

The **EUvsDisinfo** website, run by EU East StratCom, also plays an important educational role. In addition to a database with identified examples of Russian disinformation, analyses, and reports, users can also find an e-learning course, educational videos and an explanation of techniques used by Russia to disinform the public. The website has 12 language versions, which expands the audience especially to Eastern European countries. The lack of an Indian version, as well as languages of Global South countries, limits the reach to their societies. EUvsDisinfo is dedicated exclusively to countering Russian disinformation. Similar platforms dedicated to China would increase the situational awareness of FIMI threats generated by this actor.

2.2.4 International cooperation

Due to the transnational nature of information flows, international cooperation plays an important role in detecting and countering foreign disinformation operations. While the EU focuses on coordination and information-sharing among its 27 Member States, it has tools and platforms for strengthened dialogue on disinformation with third countries. Among the most important ones is the **Rapid Alert System (RAS),** which is used to exchange information on disinformation threats with partners from the G7 and NATO, or the **European Centre of Excellence (EoC) in Helsinki** for countering hybrid threats and providing training for experts from NATO and EU countries.

Despite this, EU cooperation with India on disinformation has been limited to date, as it was not recognised as important for the two sides. The ongoing **EU-India Digital Dialogue**, which met for the seventh time in October 2023, is one avenue for a possible discussion on this issue, although it is mostly known for other topics.[40] More hopes for change can be linked to the establishment in 2022 of the **EU-India Trade and Technology Council**, which deals partly also with the broad area of the digital transformation. At the first Trade and Technology Council (TTC) meeting in May 2023, the Working Group 1 on Strategic Technologies, Digital Governance, and Digital Connectivity was established, which may include a focus on the problem of

[40] Seventh India-EU Cyber Dialogue, Ministry of External Affairs, Government of India, 06 October 2023.

disinformation[41]. Still, the exchange of ideas, information, and best practices in this area between experts and officials is rather unrealised. Digital cooperation has been discussed more as an area of economic and technological progress and in terms of regulation of this relatively new area, with less attention paid to the threats of disinformation and foreign interference in the digital space.

[41] India-EU Joint Statement 1st Meeting of the Trade and Technology Council, Ministry of External Affairs, Government of India, 16 May 2023.

3. Indian Vulnerability to Foreign Disinformation and Propaganda

In India, there is an asymmetry of disinformation activities from external actors. **A greater awareness of Chinese hybrid threats prevails in India,** while Russia is perceived as a partner rather than a challenge in the sphere of information confrontation.

Awareness in recent years of disinformation from China grew after the Dokhlam standoff between the Indian and Chinese armies in 2017. That event was a watershed moment that brought to the forefront China's attempts to influence public opinion in India. According to India's security community, some journalists and social-media influencers sought to project and amplify Beijing's narrative of the 2017 standoff[42]. China's efforts were not just limited to influencing public opinion but also India's defence preparedness during that phase. Lt. Gen. Vinod Khandare, principal adviser in the Ministry of Defence, cites labour unrest in ordinance factories over the issue of "corporatisation" as a case in point[43].

The clashes in Galwan in 2020 that led to the deaths and injury of Indian and Chinese soldiers led to a serious deterioration of relations between the two states and **further attracted attention to Chinese interference in the information domain in India**. Gen. Narasimhan, who headed the Indian Ministry of External Affairs think tank on China, points towards China's use of fake videos that portray significant territorial gains in Arunachal Pradesh, a claim debunked by the Indian Army. China's aim appears to have been to create the false perception that the People's Liberation Army (PLA) has superior fighting capabilities vis-á-vis India, and to shape public discourse within India. This has alarmed the Indian strategic community and helped it to recognise the disinformation threat from China.

While Chinese influence operations have been recognised, there is no interest in India in examination of Russia's activities in the same vein. This may be in part because Russia is perceived in India as friendly country and not considered as a

[42] Interview with Jayadeva Ranade, Member of India's National Security Advisory Board and President of the Centre for China Analysis And Strategy, New Delhi, 13 June 2023.
[43] Interview with Lt. Gen. Vinod G. Khandare (retd), Principal Advisor, Ministry of Defence, Government of India, New Delhi, 20 June 2023.

source of inimical behaviour. The Russian narrative on international affairs, including on the conflict in Ukraine, is seen as a justified way to present its perspective and not as a challenge. As a result, **Indian policymakers and experts do not focus on Russian disinformation in this sense and focus exclusively on China's activities**.

An interesting point of analyses is the distinction between the Chinese and Russian disinformation tactics: first, when one looks at China, the country presents an information black hole to the world, while for its population it is also the most restrictive regime. **While Beijing adopted the Russian rulebook on disinformation, its tactics have evolved in the past few years, with the differences largely based on the required outcomes.** Chinese information campaigns aim first to uphold a single narrative that puts the CCP in a positive light; second, it seeks to censor information and suppress dissenting narratives outside China; third, it is not utilised to destabilise the information environment as much as it is to present China in a positive light. What makes it different from Russia's is that the Chinese strategies do not target foreign societies beyond creating positive perceptions of China. These tactics have been used by Beijing to create an alternative narrative in India, as detailed in the following sections.

3.1. What Does China Target India on?

China's disinformation strategy in India is in line with its global objectives of promoting certain key areas and issues that are essential to the future of the Chinese Communist Party and the image of China as a "modern, unified, and globally powerful nation".[44] Dexter Roberts suggests two core areas – both of which are particularly relevant to India:

- ✓ The first, is protecting China's inviolate national sovereignty – especially in areas like Xinjiang, Tibet, Hong Kong, and Taiwan.[45] This is of particular relevance to India given the land border it shares with China across its north and north-east region. These include the Union Territory of Ladakh, and the North-Eastern states of Arunachal Pradesh and Sikkim[46] – which share

[44] Dexter Roberts, "China's Disinformation Strategy", Atlantic Council, Washington DC, 2020, https://www.atlanticcouncil.org/wp-content/uploads/2020/12/CHINA-ASI-Report-FINAL-1.pdf.
[45] Ibidem.
[46] Ananth Krishnan, correspondent for *The Hindu*, and author of the book *India's China Challenge* highlights how the Dokhlam incident marked a new Chinese approach with regard to its engagement on future border crises. The PLA daily termed this approach an "information warfare strategy" that aimed

borders with China. In addition, this would also include concerns over the Chinese region of Tibet, given that the Dalai Lama resides in India.

- ✓ The second, is promoting China as a strong, stable, and leading country.[47] China is keen to promote itself as a global leader and the regional power in Asia. Within this context – India becomes a potential opponent. Stifling Indian economic growth and "slowing down of its pace"[48], underrating Indian democracy (the world's largest)[49] and political system, and creating cleavages within Indian cultural communities[50] is crucial to promote China's economic prowess, the success of the Chinese one-party system, and China's push to stifle identity-based movements in its own country.[51]

Also authors of a report published by the International Republican Institute (IRI), see it as a broader "information shaping/manipulating" approach, and not just as a misinformation or disinformation operation.[52] The report suggests that for China, the ability to successfully manipulate information spaces in the Indo-Pacific is vital for their regime security.[53] Therefore China focuses on countering perceived challenges around its periphery – including the South China Sea territorial disputes and the disputes in the Himalayan borders it shares with India.[54] It also wants to create an

---

to "fully integrate the public forces" of various forms of media in order to carry out a "multi-wave and high-density centralised publicity in a fixed period of time" with the end goal being creating favourable public opinion. He also brings attention to the PLA's Western Theatre Command's 2017 analysis of the Dokhlam media strategy. Which said that "seizing the initiative key in a struggle for public opinion" with the ultimate aim "to make India succumb without a confrontation". For details see: Ananth Krishnan, *India's China Challenge* (New Delhi: Harper Collins Publishers India, 2020), p. 212.

[47] Dexter Roberts, "China's Disinformation Strategy", Atlantic Council, Washington DC, 2020, https://www.atlanticcouncil.org/wp-content/uploads/2020/12/CHINA-ASI-Report-FINAL-1.pdf.

[48] Interview with Lt. Gen. (ret.) Vinod G. Khandare, Principal Advisor, Ministry of Defence, Government of India, New Delhi, 20 June 2023.

[49] Dr. Sriparna Pathak, Associate Professor and Associate Dean of Admissions at the Jindal School of International Affairs highlights that Chinese DPM efforts have been used to characterise India as not a true democracy.

[50] Lt. Gen. Khandare suggests that India's biggest weakness is its internal cohesion.

[51] Jayadeva Ranade suggests that there is also an effort by China to create a sense of defeatism amongst other countries. Calling it a "broad-brush" campaign that incorporates both misinformation and propaganda, China seeks to push a perception that it is highly advanced both to create a sense of intimidation in other countries on China's proves (this has been often seen on the military front) and to create a sense that their own countries would never be able to meet China's standards, no matter what they did.

[52] International Republican Institute, *"Countering China's Information Manipulation in the Indo-Pacific and Kazakhstan",* Washington DC, International Republican Institute, 2023, https://www.iri.org/resources/countering-chinas-information-manipulation-in-the-indo-pacific-and-kazakhstan/

[53] Ibidem.

[54]Ibidem.

acceptance of its preferred narrative as this is deeply linked to its security and economic objectives in the Indo-Pacific.[55]

In this context, **main topics and messages disseminated by China refers to India as a growing competitor and has to depict China as superior in all domains**. Firstly, information manipulation around the Dokhlam and Galwan clashes, as said earlier, were to present China as militarily stronger. Secondly, rapid economic rise of India coupled with the slowdown in China raised an anxiety of being dethroned and has led to China bolstering its own image, as evidenced from Communist regime's reaction that "quality of the workforce matters, not quantity" as India's population overtook China's.[56] China also targets the renewable-energy sector in India through disinformation campaigns. A nation's demand for energy goes up as its economy prospers. China's aims are that crippling Indian's Energy capacity will dent its economy. Thus, there is an attempt to stymie India's development trajectory, which can be evidenced from General Khandare's assertion that while China is on a spree to build hydropower projects along with its border with Arunachal Pradesh, it has been stoking opposition to such initiatives in India. Moreover, there are also reports that China uses its influences in Asian Infrastructure Investment Bank against India. Dr. Jabin Jacob, from Shiv Nadar University, claims that Indian membership in AIIB makes the CPC gaining crucial insights into Indian economic interests since it can access dealings between the lending institution and Indian state.[57] Accessing such privileged information regarding a rival helps China to devise more targeted disinformation measures to hobble the Indian economic initiatives.

Thirdly, China's disinformation take an aim at Indian political system. Aadil Brar suggested that China's operations target India's society and economy, with a "goal to project India's democracy as dysfunctional"[58]. He further goes on to suggest that while media and policy makers focus more on disinformation within the context of particular border skirmishes, there is also the projection of India's democratic institutions as

[55] Ibidem.
[56] "China jibes about 'quality' as India becomes the world's most populous country," *The Mint*, April 20, 2023, https://www.livemint.com/news/india/china-jibes-about-quality-as-india-becomes-world-s-most-populous-country-11681988806133.html
[57] Jabin T Jacob, "New Delhi's approach to multilateral ties needs clarity," *The Mint*, June 26, 2023, https://www.livemint.com/opinion/columns/new-delhi-s-approach-to-multilateral-ties-needs-clarity-11687799731053.html
[58] Questionnaire Response by Adil Brar, Journalist and a Visiting Scholar at the National Chengchi University, Taiwan.

weak, questions over India's diplomatic ties with the United States, and the emphasis on India as a hegemon in South Asia".[59] Lt Gen S Narasimhan[60] also highlights India's democratic nature, and adds questions on performance of the manufacturing sector, doubts surrounding the capabilities of the Indian Army in comparison to the Chinese PLA, and social issues.

Finally, there is also an **element of civilizational competition in Chinese disinformation**. Both the security and academic communities in India identify Chinese pushing the narrative of its rise in the Indian media space. Prof. Sreeparna Pathak, Jindal School of International Affairs of O.P. Jindal Global University, homes in on China's use of Mandarin-learning online platforms that promote the idea of "Chinese exceptionalism" and "superiority of its civilisation". Ranade endorses that some Indian newspapers publish news reports on China's scientific achievements, but they are depicted in such a way as to induce a perception of defeatism within the Indian public community.

3.2. On What Issues Does China target India?

China uses a variety of platforms, means, and methods to spread disinformation and manipulate Indian public. Though it is part of China's global strategy to strengthen its discourse power[61], it has several elements specific to the Indian context. The main tools and techniques are presented in the following sections.

3.2.1 Social Media platforms

India has been especially vulnerable to disinformation through social media due to deep penetration of the Indian market by Chinese platforms. Unlike globally where the crux of China's foreign direct investment (FDI) lies in physical infrastructure through the Belt and Road Initiative, in India, the core of China's investment is in the software and internet sector. According to a report by Gateway House titled "Chinese

[59] Ibidem.
[60] Online Interview with Lt Gen SL Narasimhan is former Director General at the Centre for Contemporary China Studies, 22 June 2023.
[61] International Republican Institute, *"Countering China's Information Manipulation in the Indo-Pacific and Kazakhstan",* Washington DC, International Republican Institute, 2023, https://www.iri.org/resources/countering-chinas-information-manipulation-in-the-indo-pacific-and-kazakhstan/;
Paul Scharre, *The Dangers of the Global Spread of China's Digital Authoritarianism,* Washington DC, Center for a New American Security. 2023, https://www.cnas.org/publications/congressional-testimony/the-dangers-of-the-global-spread-of-chinas-digital-authoritarianism.

Investment in India", in 2020, Chinese tech investors put an estimated $4 billion into Indian startups, resulting in 18 of India's 30 unicorns to be Chinese-funded[62]. These include not just smartphone apps but also the physical devices on which these applications run[63]. This change of strategy has allowed Chinese funding to the Indian tech sector to make an impact disproportionate to its value[64]. In 2018, the top 50% of smartphone applications downloaded in India were those with Chinese investment[65]. In 2019, Chinese smartphone manufacturers enjoyed a 66% share of the Indian smartphone market[66]. This presence is particularly of concern in three specific areas[67]:

- ✧ **Data Security –** Chinese investments into Indian companies allow the parent company the opportunity to access the data of Indian users[68]. This data can be mined, especially with the advent and accessibility of artificial intelligence (AI) to create targeted, bespoke efforts of the second type of concern—propaganda, influence, and censorship.
- ✧ **Propaganda, influence, censorship –** Recent reports have confirmed what many feared about Chinese software behemoth TikTok—that it subtly pushes a Chinese narrative. For India specifically, this may include a narrative shift on bilateral issues and disputes to one creating a more favourable depiction of China and suppressing criticism antithetical to Chinese interests[69].
- ✧ **Platform Control –** With Chinese investment present as the leader in most categories of applications in India, there is the potential for a future event of Chinese platform control of such applications. This would be of particular concern especially for applications that deal with location information (food

[62] Amit Bhandari, Blaise Fernandes, Aashna Agarwal, *"Chinese Investments in India,* Gateway House, February 2020, https://www.gatewayhouse.in/wp-content/uploads/2020/07/Chinese-Investments_2020-Final.pdf.
[63] Ibidem.
[64] Ibidem.
[65] Ibidem. One factor to this market share is that many Chinese applications come designed as utility apps (smartphone battery optimizer, memory optimiser, etc).
[66] Amit Bhandari, Blaise Fernandes, Aashna Agarwal, *"Chinese Investments in India,* Gateway House, February 2020, https://www.gatewayhouse.in/wp-content/uploads/2020/07/Chinese-Investments_2020-Final.pdf.
[67] Ibidem.
[68] Several companies do suggest that the data are stored locally in India, and that the parent company in China has no access to the data.
[69] Amit Bhandari, Blaise Fernandes, Aashna Agarwal, *"Chinese Investments in India,* Gateway House, February 2020, https://www.gatewayhouse.in/wp-content/uploads/2020/07/Chinese-Investments_2020-Final.pdf.

delivery, travel apps), payment systems (UPI, net banking apps), and information dissemination (audio, video, radio apps).

While the Indian government does not allow for FDI in or ownership of newspapers and news channels, news applications do not have such limitations. These investments thus are particularly concerning since it allows China the opportunity to closely influence and moderate the news Indians read.

3.2.2 Opinion Makers

Through several efforts, China attempts to "influence" and befriend those whose opinions could and often do impact a significant cross-section of Indian society. These include journalists, professors, students, and bureaucrats. These operations have been considered similar to the previous influence operations conducted by the KGB and GRU, with the difference that China has increased the level of sophistication involved[70].

3.2.3 Education and Research

According to Jayadeva Ranade, the majority of Chinese narratives in India emerge through academia. Education and research by far can be argued to be the widest—and also deepest—extent of Chinese investment in India. China has offered grants to universities, think tanks, and advocacy groups, and also organised scholarships and study centres. There is additionally also investment in online education platforms[71].

3.2.4 Entertainment Sector

There has been a global effort by China to influence mediums of entertainment, especially film and television. This exercise has been observed in Hollywood and also in a part of the Indian entertainment industry. In 2018, the regulation of film and media in China was handed over to the propaganda department of the CCP, including control of the Chinese International Film Festival[72]. The next year, the festival saw the 2018 China-India Film Co-Production Dialogue[73]. A large amount of Chinese funds are also

[70] Suggested by Jayadeva Ranade, Former Member of India's National Security Advisory Board and President of the Centre for China Analysis And Strategy, New Delhi, during an interview on 13 June 2023.
[71] "Mapping Chinese Footprints and Influence Operations in India", Law and Society Alliance, 3 September 2021, https://tibet.net/wp-content/uploads/2021/09/MAPPING-CHINESE-FOOTPRINTS-AND-INFLUENCE-OPERATIONS-IN-INDIA2.pdf.
[72] Ibidem.
[73] Ibidem.

invested in film and TV applications in India. For instance, Xiaomi and TenCent have invested in entertainment apps, OTT platforms, and radio channels[74].

3.3. Resilience to disinformation in India

In the aftermath of the 2020 Galwan clashes, India went about systematically curbing instruments that China uses to expand its influence[75]. In the following months, the **government banned nearly 300 Chinese phone apps**, chief among them the short video-hosting service TikTok[76]. It has also reviewed 54 memoranda of understanding signed between Indian universities and China on Confucius Institutes and educational cooperation between higher education institutions. Guidelines related to such collaborations have been tightened and will require government clearance, with educational joint ventures with Chinese entities brought under the purview of the stringent legislation regulating foreign funding[77]. More recently, the government reduced the period of visas for Chinese journalists who were found visiting Tibetan settlements without applying for the requisite permission, and did not renew visas for them in 2023, leaving China practically without any correspondent in India[78].

In addition to these technical and administrative decisions, **India has also strengthened resilience in legal terms**. Thus far, rights and responsibilities of online platforms (also in the context of defamation and creating disharmonious situations) were regulated by the Information Technology Act of 2000, which under its Section 79 makes[79] a clear reference to due diligence on the part of network service providers to remove or disable access to illegal or false information. **The 2021 IT rules** that

[74] Ibidem.
[75] Online Interview with Lt. Gen. SL Narasimhan is former Director General at the Centre for Contemporary China Studies, 22 June 2023.
[76] "China cries foul as govt reviews presence of Confucius centres," Times of India, August 5, 2020, https://timesofindia.indiatimes.com/india/china-cries-foul-as-govt-reviews-presence-of-confucius-institutes/articleshow/77362406.cms; Divya Bhati, "Full list of Chinese apps banned in India so far: PUBG Mobile, Garena Free Fire, TikTok and hundreds more," *India Today*, August 21, 2022, https://www.indiatoday.in/technology/news/story/bgmi-garena-free-fire-tiktok-and-more-banned-in-india-check-the-full-list-1990048-2022-08-19,
[77] "India makes FCRA clearance mandatory for tie-ups with China's Confucius Institutes," Indian Express, April 29, 2022, https://indianexpress.com/article/education/india-makes-fcra-clearance-mandatory-for-tie-ups-with-chinas-confucius-institutes-7891399/.
[78] Ananth Krishnan, "China says its reporters in India 'about to drop to zero' amid mutual expulsions," *The Hindu*, June 1, 2023, https://www.thehindu.com/news/international/china-says-its-reporters-in-india-about-to-drop-to-zero-amid-mutual-expulsions/article66920412.ece.
[79] Section 79 in The Information Technology Act, 2000,https://indiankanoon.org/doc/844026/#:~:text=(1)per cent20Notwithstandingper cent20anythingper cent20containedper cent20in,availableper cent20orper cent20hostedper cent20byper cent20him.

replaced the previous guidelines have sought to further regulate social media platforms. **The amendments introduced in April 2023** give the government sweeping powers to exercise censorship and also call on social and media platforms to remove posts deemed fake or false. This new Act is also expected to ensure data privacy, net neutrality, and most importantly, accountability of social media platforms, including X (formerly Twitter), YouTube, and Facebook (Meta)[80].

Yet, Chinese propaganda tries to seep through the cracks. A recent *New York Times* investigation revealed that a U.S. businessman settled in Shanghai has been using social media networks and funnelling funds into online news platforms that have been spreading the CPC's message in India[81]. This has led people in the security community to pitch for more reforms to combat Chinese disinformation. However, government regulations for the media are a non-starter, since that would invoke the spectre of censorship of the Fourth Estate.

Thus, the **security community has proposed a broad response to Chinese disinformation**: one, an institutional mechanism to counter Chinese propaganda, two involving people. Gen. Narasimham supports the creation of an agency that can identify propaganda and respond to it promptly. Gen. Khandare takes this concept forward by batting for structural reforms in which the Information and Broadcasting Ministry is given a seat on the Cabinet Committee on Security to ensure that it is able to proactively counter propaganda. He also cites Prime Minister Narendra Modi's idea of involving the national volunteer youth corps—National Cadet Corps and National Service Scheme—in efforts to combat fake news. Yet, the discussions are inconclusive as for now **India is still searching for a more effective way to strengthen response to foreign interference and resilience to disinformation**. This may, actually open the opportunity for closer collaboration with the EU on the subject.

[80] Soumyarendra Barik, "New IT Act looks to rein in 'deliberate' misinformation", The Indian Express, 15 July 2022, https://indianexpress.com/article/technology/tech-news-technology/new-it-act-looks-to-rein-in-deliberate-misinformation-8027748/.

[81] Mara Hvistendahl, David A. Fahrenthold, and others, "A Global Web of Chinese Propaganda Leads to a U.S. Tech Mogul," *New York Times*, August 5, 2023, https://www.nytimes.com/2023/08/05/world/europe/neville-roy-singham-china-propaganda.html.

4. Conclusion and Recommendations: Towards an EU-India Joint Response to Disinformation

Foreign disinformation and manipulation in information domain has emerged as a serious threat to both the European Union and India in recent years. As India-EU strategic partnership is getting stronger and wider, a **dialogue on disinformation can prove helpful to both sides.** It could pave the way for better understanding and strengthening of resilience to deal with a new challenge. India and the EU can work towards understanding the nature of the threat, design tools for countering disinformation, jointly draft working methods to address the risks, formulate responses and improve resilience. This could not only strengthen their strategic partnership but can be a starting point for a global discussion on the regulation of disinformation.

This report made some initial insights into the comparison of the EU and India's dealings with disinformation. It reveals both some important similarities and striking differences in the EU and India's approaches to this threat. **While this must be seen as a first step in better understanding of this issue and more in-depth studies are encouraged**, it allows for drawing preliminary conclusions.

First of all, one must stress that **there is no common understanding and definition of disinformation between the EU and India**. This may lead to different threat assessments and misunderstandings between the two when it comes to specific responses or attempts at international regulation of this domain. It may potentially spark some controversies regarding acceptable and preferable methods of countering disinformation, and feed into mistrust. Therefore, it points at the necessity of a more regular and deepened dialogue between the EU and India on this issue.

Second, **there is a discrepancy in how the two actors see the source and threat of disinformation** linked, among others, to the historical and geographical context of the two. While the EU recognised this threat following the Russian aggression in Ukraine in 2014, it was the Dokhlam clashes in 2017 (and even more so the Galwan border clashes in 2020) with China that served as the wake-up call for India. As a result, **the EU identifies Russia as a major threat in the information domain** and started to pay more attention to Chinese behaviour only recently, while **India focuses exclusively on Chinese activities** in this regard. This discloses their different

perspectives and may feed into mutual suspicion on the one hand, but also offers a lot of potential for mutual learning and sharing of experience and lessons learnt in dealing with disinformation. **While the EU has accumulated a better understanding and knowledge of Russian FIMI in Europea, India seems more exposed to Chinese activities in this regard**. As European experience indicates, China is still learning from Russia how to apply disinformation more aggressively in its foreign operations, and this may be a valuable observation for India. **If it wants to prepare better for more sophisticated Chinese operations in the future, it should study Russian disinformation in Europe for its own interest.**

Third, both the **EU and India have already developed a certain counter-disinformation toolbox consisting of legal, institutional, and educational tools enabling to bolster social resilience**. They have undertaken even some similar steps to limit foreign manipulation operations, including banning certain news outlets (Russian media, like RT in the EU; Chinese news apps, like TikTok in India) and journalists (in fact propagandists), curbing operations of cultural institutions (e.g., Confucius Institutes), and limiting the space for certain opinion leaders. At the same time, **the EU seems a more advanced actor when it comes to conceptualisation (e.g., the official definition of FIMI) and institutionalisation of preparedness to disinformation (establishment of mechanisms like East StratCom, or regulations like the DSA).** India, which is planning its own institutions and mechanisms for monitoring and countering disinformation may be interested in consulting of some ideas and getting support from the EU in this regard. And **as both sides are still searching for most effective ways to address this challenge there is great scope for cooperation** in the preparation of new tools and mechanisms to counter disinformation, raise public awareness about the threat, and harmonise their legal, administrative, and educational response.

One needs to remember that combating disinformation in democratic states has its legal, political, and social limitations. The use of such legal instruments as sanctions on individuals or entities (e.g., media) are measures of last resort. In democratic states, freedom of expression is a fundamental right. Disinformation perpetrators often use the privileges of democracy to undermine it, claiming that they have the right to make “claims” on the basis of this right. In such circumstances, it is difficult to punish or publicly stigmatise those responsible for creating, reproducing, and disseminating

manipulated or false information. In this context, closer cooperation, information-sharing and best practices on countering disinformation may bring mutual benefits to both India and the EU boosting their preparedness to foreign interference and enhancing mutual trust.

Finally, while the **European Union engages third countries in collaboration on disinformation, this aspect of relations with India is strikingly missing**. Yet, several EU institutions or EU-funded projects and mechanisms can potentially be of interest to its Indian counterparts.

This study points at the great untapped potential for discussion and cooperation between the EU and India in dealing with this emerging threat. **The upcoming general elections in India and the EU in 2024 and the critical role of digital infrastructure make the case for strengthened collaboration more urgent.** Therefore, to boost cooperation in this area the following recommendations can be considered.

4.1. Recommendations for the EU and India:

- **Launch a formal and specialised Disinformation Dialogue** within the existing institutional framework to narrow the differences and work out a common understanding and responses to disinformation threat. This can be included as part of the **EU-India Cyber Dialogue**, or more ambitiously, as part of the **EU-India Trade and Technology Council**[82], where a Task Force can be formed specifically on disinformation in the digital space under Working Group 1. This task force could **prepare a threat assessment on disinformation before the upcoming elections in the EU and India in 2024 to be presented by the next TTC meeting**.
- **Open up the EU Rapid Alert System** (RAS) **to cooperation with India** to facilitate the regular sharing of insights related to disinformation campaigns on the internet and coordinate responses. Alternatively, they could consider forming a **Bilateral Rapid Response Team** to quickly address emerging disinformation threats, particularly during critical events like elections or public health crises.
- To mitigate the risks of foreign interference and manipulation in the upcoming elections in the EU and India in 2024 prepare and **launch ahead of the polls a joint Public Awareness Campaign** on digital and traditional media to educate the public about disinformation, its impact, and ways to identify and minimise it.

[82] M. Makowska, *EU Agrees the Digital Services Act*, “PISM Bulletin”, 16 May 2022, www.pism.pl.

- Invest in capacity-building and societal resilience by launching a special **programme to provide and organise reciprocal study visits for journalists, experts, officials, and practitioners from India and the EU** to exchange and deliberate on best practices in terms of countering disinformation. It is especially important to support independent journalists and media houses in both regions to strengthen investigative journalism and fact-checking capabilities. The programme can be coordinated on the EU side by the Strategic Communication team at the EEAS and funded from the International Partnership Instrument under the MFF 2022-2027.
- **Continue discussions on regulation of the internet and digital space** in international relations and promote best standards and practices to limit the disinformation threats. For this, the EU could exchange opinions with Indian partners under the EU-India Technology and Trade Council about the barriers and possibilities to introduce similar rules to the European Digital Services Act.
- **Support Joint Research and Development Initiatives** to develop advanced technologies such as AI and machine learning tools to more effectively detect and counter disinformation.

4.2. Recommendations for the EU:

- Continue investing in strengthening its own institutions and resilience to disinformation and **consider establishing of a new special Asia StratCom unit at EEAS (or India StratCom, Indo-Pacific StratCom)** to better monitor the disinformation threats in India and its region. This task force would be a natural partner for cooperation, training, and exchange of information with Indian counterparts.
- **Support technically and financially (from the Horizon Europe programme or International Partnership Instrument) the creation of a Centre for Excellence for Countering Disinformation and Hybrid Threats in New Delhi** (like the CoE in Helsinki) as an academic hub for research and collaboration between Indian and European experts in this field, to increase awareness and the capacity to deal with disinformation in Indian society.
- **Launch a special "EU-India Disinfo Lab" platform** that would bring together disinformation experts and academic communities, fact-checking organisations, NGOs, civil society, etc. from India and EU countries. Given the EU's experience

with Russian disinformation and India's experience with disinformation from China, such a knowledge-sharing platform would increase the situational awareness of both actors.

- **Extend the mandate of EUvsDisinfo** or create a new similar platform to monitor disinformation threat in the EU coming from China.
- Continue supporting further academic cooperation and research on disinformation in India from China and Russia, possibly through **new calls for proposals under the EU-India Think Tank Twinning Initiative.**

4.3. Recommendations to Indian government:

- **Consider the establishment of an official structure within the government** (an agency, a working group or a task force similar to EU StratCom) **as kind of an early-warning system for disinformation**, to monitor, analyse, and share information on foreign influence operations in the country.
- **Invest in societal awareness and resilience to disinformation threats by supporting academic and civil society initiatives** working in this field. Some initiatives developed already in the EU, like the **European Digital Media Observatory (EDMO), or the EUvsDisinfo platform** may serve as points of reference for developing a pan-Indian network of experts and practitioners monitoring emerging threats and educating the society.
- **Engage the European partners in open dialogue on disinformation within the EU-India TTC and other platforms in order to shape the global regulation on disinformation.** As part of it, support civil-society exchanges and research on the topic.
- **Analyse Russian disinformation operations in the EU to learn and prepare for more advanced Chinese operations in India in the future.** Consider examining Russian campaigns in information domain in India also through the prism of disinformation and be open to engage the EU in dialogue and information-sharing on all relevant FIMI threats.

5. Annexes

ANNEX 1

Bibliography

ANNEX 2

List of Interviews

Annex 1

Bibliography

- "China cries foul as govt reviews presence of Confucius centres," *Times of India*, August 5, 2020, https://timesofindia.indiatimes.com/india/china-cries-foul-as-govt-reviews-presence-of-confuciusinstitutes/articleshow/77362406.cms
- "China jibes about 'quality' as India becomes the world's most populous country," *TheMint*, April 20, 2023, https://www.livemint.com/news/india/china-jibes-about-quality-as-india-becomes-world-s-most-populous-country-11681988806133.html
- "Distinguishing Disinformation from Propaganda, Misinformation, and 'Fake News'", Digital Forensic Centre, https://dfcme.me/en/distinguishing-disinformation-from- propaganda-misinformation-and-fake-news/
- *2021 StratCom activity report - Strategic Communication Task Forces and InformationAnalysis Division*, 24 March 2022 r., www.eeas.europa.eu.
- Adjin-Tettey T.D., *Combating fake news, disinformation, and misinformation: Experimental evidence for media literacy education*, Cogent Arts & Humanities (2022),9: 2037229, DOI:10.1080/23311983.2022.2037229.
- Alex Joske, Spies and Lies: How China's Greatest Covert Operations Fooled the World,Hardie Grant, 2022.
- Amit Bhandari, Blaise Fernandes, Aashna Agarwal, "Chinese Investments in India, Gateway House, February 2020, https://www.gatewayhouse.in/wp-content/uploads/2020/07/Chinese-Investments_2020-Final.pdf
- Ananth Krishnan, "China says its reporters in India 'about to drop to zero' amid mutualexpulsions," *The Hindu,* June 1, 2023,https://www.thehindu.com/news/international/china-says-its-reporters-in-india-about- to-drop-to-zero-amid-mutual-expulsions/article66920412.ece
- Bagge D., *Unmasking Maskirovka: Russia's Cyber Influence Operations*, DefensePress, New York 2019.
- Barbashin A., Graef A., *Thinking Foreign Policy in Russia: Think Tanks and Grand Narratives*, www.atlanticcouncil.org/wp-content/uploads/2019/11/Thinking-Foreign- Policy-in-Russia_- Think-Tanks-and-Grand-Narratives-Atlantic-Council-11.12.19.pdf
- Bradshaw, Samantha and Howard, Philip N., "The Global Disinformation Order: 2019Global Inventory of Social Media Manipulation" (2019).
- Bryjka F., *Detecting and Countering Disinformation - A Proposal for a Syllabus for a University Course*, [in]: R. Kupiecki, A. Legucka (ed), Disinformation and the Resilience of Democratic Societies, PISM, Warsaw 2023.
- Bryjka F., *Tracing the Development of EU Capabilities to Counter Hybrid Threats*, "PISM Strategic File", No. 9, 1 August 2022, www.pism.pl.
- Chłoń T., Kozłowski K., *Selected Case Studies of Systemic Disinformation: Russia and China*, in: R. Kupiecki, A. Legucka, *Disinformation and the Resilience of Democratic Societies*, PISM, Warsaw 2023.
- *Civic Resilience Course*, www.debunk.org.
- Collier K., *China-based Covid disinformation operation pushed fake Swiss scientist, Facebook says*, 1 December 2021, https://www.nbcnews.com

- *Council Regulation (EU) No 269/2014 of 17 March 2014 concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine*, 17 March 2014, www.eur-lex.europa.eu.
- Czerep J., Nowacka S., *Fertile ground: How Africa and the Arab World found commonlanguage with Russia on Ukraine*, "PISM Report", 17 January 2023, www.pism.pl.
- Dexter Roberts, "China's Disinformation Strategy", Atlantic Council, Washington DC, 2020, https://www.atlanticcouncil.org/wp-content/uploads/2020/12/CHINA-ASI-Report-FINAL-1.pdf.
- DiResta R., Grossman Sh., *Potemkin pages and personas. assessing GRU onlineoperations 2014−2019*, Stanford University, Stanford 2019.
- Divya Bhati, "Full list of Chinese apps banned in India so far: PUBG Mobile, GarenaFreeFire, TikTok and hundreds more," *India Today*, August 21, 2022, https://www.indiatoday.in/technology/news/story/bgmi-garena-free-fire-tiktok-and- more-banned-in-india-check-the-full-list-1990048-2022-08-19
- *EU imposes sanctions on state-owned outlets RT/Russia Today and Sputnik's broadcasting in the EU*, Council of the EU Press release, 2 March 2022, www.consilium.europa.eu.
- European External Action Service (EEAS). October 2021. "Tackling Disinformation, Foreign Information Manipulation and Interference. StratCom Activity Report." https://www.eeas.europa.eu
- European External Action Service, *1st EEAS Report on Foreign Information Manipulation and Interference Threats Towards a framework for networked defence*, Strategic Communications, Task Forces and Information Analysis (STRAT.2), February 2023, [online] https://euvsdisinfo.eu
- European External Action Service, *1st EEAS Report on Foreign Information Manipulation and Interference Threats Towards a framework for networked defence*, Strategic Communications, Task Forces and Information Analysis (STRAT.2), February 2023, [online] https://euvsdisinfo.eu
- *European Parliament resolution of 9 March 2022 on foreign interference in all democratic processes in the European Union, including disinformation*, 9 March 2022,https://www.europarl.europa.eu
- Giles K., *Handbook of Russian information warfare*, NATO Defence College Fellowship Monograph, 9, Rome 2016, www.ndc.nato.int/news/news.php?icode=995
- Giles K., Sherr J., Seaboyer A., *Russian reflexive control*, Royal Military College of Canada, Kingston 2018.
- Helmus T.C., *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe*, RAND Corporation, Santa Monica 2018, www.rand.org/pubs/research_ reports/RR2237.html
- *How the EU responds to crises and builds resilience*, European Council, 28 October 2023, www.consilium.europa.eu.
- *Image control: How China struggles for discourse power*, "Merics", 27 September 2023,www.merics.org

- Innocent E. Chiluwa and Sergei A. Samoilenko (editors), Handbook of Research on Deception, Fake News, and Misinformation Online, 2019
- International Republican Institute, "Countering China's Information Manipulation in the Indo-Pacific and Kazakhstan", Washington DC, International Republican Institute,2023, https://www.iri.org/resources/countering-chinas-information-manipulation-in- the-indo-pacific-and-kazakhstan/
- Isaac Stone Fish, America Second: How America's Elites Are Making China Stronger,Knopf, 2022.
- Jabin T Jacob, "New Delhi's approach to multilateral ties needs clarity," The Mint, June 26, 2023, https://www.livemint.com/opinion/columns/new-delhi-s-approach-to- multilateral-ties-needs-clarity-11687799731053.html
- Journalism, 'Fake News' & Disinformation - Handbook for Journalism Education and Training", United Nations Educational, Scientific and Cultural Organization, 2018, https://en.unesco.org/sites/default/files/journalism_fake_news_disinformation_print_friendly_0.pdf
- Kurlantzick J., *How China Ramped Up Disinformation Efforts During the Pandemic*, "Council on Foreign Relations", 10 September 2020,https://www.cfr.org/in-brief/how-china-ramped-disinformation-efforts-during- pandemic
- Legucka A., Przychodniak M., *Disinformation from China and Russia during theCOVID-19 Pandemic*, "PISM Bulletin", 21 April 2020, https://pism.pl/
- Makowska M., *EU Agrees the Digital Services Act*, „PISM Bulletin", 16 May 2022, www.pism.pl.
- Mapping Chinese Footprints and Influence Operations in India", Law and Society Alliance, 3 September 2021, https://tibet.net/wp-content/uploads/2021/09/MAPPING- CHINESE-FOOTPRINTS-AND-INFLUENCE-OPERATIONS-IN-INDIA2.pdf
- *Media & Disinformation: a survival guide to your everyday life on the internet*, www.knowhoax.org.
- *Media Literacy Index 2021*, Open Society Institute Sofia, 14 March 2021, www.osis.bg.
- Paul Ch., Matthews M., *The Russian "Firehose of Falsehood" Propaganda Model*, RAND Corporation, Santa Monica 2017, www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE198/RAND_PE198.pdf
- Paul Scharre, The Dangers of the Global Spread of China's Digital Authoritarianism, Washington DC, Center for a New American Security. 2023, https://www.cnas.org/publications/congressional-testimony/the-dangers-of-the-global-spread-of-chinas-digital-authoritarianism.
- Podemska J., Podemski P., *Protect Yourself Against Disinformation*, [in]: Kupiecki R.,Legucka A. (ed), Disinformation and the Resilience of Democratic Societies, PISM, Warsaw 2023.
- *Protokoł czetyrnadcatoro zasiedanija Podkomissii po sotrudniczestwu w obłasti sriedsw massowoj informacyi Rossijsko-Kitajskoj Komissii po gumanitarnomu sotrudniczestwu*, Ministerctwo cyfrowogo razwitija, swiazi i massowych

kommunikacyj Rossijskoj Fiedieracyi, 29 July 2021 https://www.documentcloud.org.

- Przychodniak M., *Chinese Disinformation: Ideology, Structures, Efficiency,* in: R. Kupiecki, A. Legucka, *Disinformation and the Resilience of Democratic Societies*, PISM, Warsaw 2023.
- Rid T., *Active Measures: The Secret History of Disinformation and Political Warfare*, Macmillan, New York 2020.
- Russia's national security strategy and military doctrine and their implications forthe EU, Directorate-General for External Policies, European Parliament, 2017:

  Russia's national security strategy and military doctrine and their implications for the EU (europa.eu).
- Russia's Strategic and Tactical Narratives in Its War against Ukraine, YouTube: Centrefor Democratic Integrity, 28 December 2022., www.youtube.com.
- Rychlak R., Pacepa I.M., *Disinformation: Former Spy Chief Reveals Secret Strategies for Undermining Freedom, Attacking Religion, and Promoting Terrorism*, WND Books,Washington 2013.
- Shekhovtsov A., *Russia and the Western Far Right*. *Tango Noir*, Routledge, New York2018.
- Shivangi Singhal, Rishabh Kaushal, Rajiv Ratn Shah, Ponnurangam Kumaraguru, 'FakeNews in India: Scale, Diversity, Solution, and Opportunities', Communications of the ACM, November 2022, Vol. 65 No. 11, Pages 80-81
- Soumyarendra Barik, "New IT Act looks to rein in 'deliberate' misinformation", The Indian Express, 15 July 2022, https://indianexpress.com/article/technology/tech-news- technology/new-it-act-looks-to-rein-in-deliberate-misinformation-8027748/
- *Strengthened Code of Practice on Disinformation 2022*, European Commission, 16 June2022, www.digital-strategy.ec.europa.eu
- Susan L. Shirk, Overreach: How China Derailed Its Peaceful Rise. New York: Oxford University Press, 2022.
- Szczudlik J., Legucka J., *Breaking Down Russian and Chinese Disinformation and Propaganda About the War in Ukraine*, „Strategic File PISM", 17 January 2023, https://pism.pl/
- The Kremlin's Trolls Never Sleep, Political Capital, 28 October 2022, www.politicalcapital.hu.
- Thompson J., Graham T., *Russian Government Accounts Are Using a Twitter Loophole to Spread Disinformation*, "The Conversation", 15 March 2022, http://theconversation.com.
- Usha M Rodrigues and Jian Xu, Regulation of COVID-19 fake news infodemic in Chinaand India, Media International Australia 2020, Vol. 177(1) 125–131
- Vanttinen P., Finland shuts down Confucius Institute amid censorship, espionageaccusations, "Euractive", 21 June 2022, euractiv.com
- Walter K., Hariharan H., *China, Russia Target Western Financial System withPropaganda and Disinformation*, "The Diplomat", 14 July 2023.

Annex 2

List of Interviews

1. Lt. Gen. SL Narasimhan, former Director General at the Centre for Contemporary China Studies (Ministry of External Affairs, India), Online Interview, 22 June 2023
2. Jayadeva Ranade, Member of India's National Security Advisory Board and President of the Centre for China Analysis And Strategy, New Delhi, 13 June2023
3. Lt. Gen. Vinod G. Khandare (ret.), Principal Advisor, Ministry of Defense,Government of India, New Delhi, 20 June 2023
4. Dr. Sriparna Pathak, Associate Professor and Associate Dean of Admissions at theJindal School of International Affairs, Online Interview, 3 July 2023
5. Aadil Brar, Journalist and a Visiting Scholar at the National Chengchi University,Taiwan, Interview conducted through Questionnaire
6. Dr. Jabin Jacob, Associate Professor, Department of International Relations and Governance Studies, Shiv Nadar University, UP, Interview conducted throughQuestionnaire
7. Interview with an EEAS staff member (MENA Strat Com Task Force), conducted by Filip Bryjka on June 20, 2023 in Warsaw. (Name withheld on request).
8. Interview with an EEAS staff member (East Strat Com Task Force), conducted by Filip Bryjka on June 21, 2023 in Warsaw. (Name withheld on request).
9. Interview with an EEAS staff member (East Strat Com Task Force), conducted by Agnieszka Legucka on 19 April 2023 in Brussels. (Name withheld on request).
10. Interview with an EU StratCom official (member of East Strat Com Task Force) conducted by Agnieszka Legucka on 16 June 2023 in Warsaw. (Name withheld onrequest).
11. Interview with a European China researcher, conducted by Agnieszka Legucka on4 July 2023 in Warsaw. (Name withheld on request).