DE-CONSPIRATOR

DETECTING AND COUNTERING INFORMATION SUPPRESSION FROM A TRANSNATIONAL PERSPECTIVE

D2.3

Capturing FIMI in Strategic and Military Doctrines of Russia and China

RSU

5/06/2025

Funded by the European Union

Project Information

ACRONYM	DE-CONSPIRATOR
TITLE	Detecting and Countering Information Suppression from A Transnational Perspective
GRANT AGREEMENT No	101132671
START DATE OF THE PROJECT	01/01/2024
DURATION OF THE PROJECT	36 months (2024-2026)
TYPE OF ACTION	Research and Innovation Action (RIA)
TOPIC	HORIZON-CL2-2023-DEMOCRACY-01-02
COORDINATOR	Ozyegin University from Türkiye
PROJECT OVERVIEW	DE-CONSPIRATOR aims to explore how FIMI is currently deployed by Russia and China over Europe, by mapping, understanding, assessing and predicting different FIMI strategies and their effects on EU Members States and Partner Countries. DE-CONSPIRATOR uses state-of-the-art research methods and works closely with stakeholders to fully understand the success factors, manifestations, and impacts of Russian and Chinese FIMI and to provide data-driven policy solutions. By integrating various data sources and developing a comprehensive, multilingual database of FIMI incidents, the project intends to shield European democracies against internal and external FIMI threats, all while safeguarding freedom of expression and journalism integrity.

Grant Agreement: 101132671 | Research and Innovation Action | 2024 – 2026 | Duration: 36 months

Topic: HORIZON-CL2-2023-DEMOCRACY-01-02. Type of Action: Research and Innovation Action (RIA)

Document Information

D2.3: Title of deliverable:	**Working Paper: Historical Evolution of TTPs**
Issued by:	RIGAS STRADINA UNIVERSITATE
Issue date:	30/06/2025
Due date:	Month 18
Work Package Leader:	EKONOMI VE DIS POLITIKA ARASTIRMALAR MERKEZI DERNEGI - EDAM

Dissemination Level

PU	Public	X
PP	Restricted to other programme participants (including the EC Services)	
RE	Restricted to a group specified by the consortium (including the EC Services)	
CO	Confidential, only for members of the consortium (including the EC)	

Version Control Sheet

Version	Date	Main modifications	Organisation
0.1	30/11/2024	First Version of the Document	RSU
0.2	29/05/2025	Feedback and comments by consortium partners have been incorporated.	RSU
1.0	5/06/2025	Final Version	RSU

Main Authors

Name	Organisation
Rati Akhalaia	UG
Ekin Balkan	EDAM
Una Aleksandra Bērziņa-Čerenkova	RSU
Javier Borràs-Arumí	CIDOB
Elizaveta Gaufman	RUG
Davit Kutidze	UG
Alexander Politov	CSD
Marina Rudyak	UHEI
Sinan Ülgen	EDAM

Quality Reviewers

Name	Organisation
Aurelio Insisa	IAI
Carme Colomina	CIDOB

Table of Contents

Executive Summary

Russia and China are leading actors in Foreign Information Manipulation and Interference (FIMI) campaigns against the EU and liberal democracies, using these strategies to protect their authoritarian regimes and advance strategic goals. Both perceive Western liberal values as existential threats, framing their actions as defensive while engaging in aggressive disinformation and propaganda to undermine democratic societies and promote their own narratives.

In contrast to the EU, which—through the EEAS—adopts a defensive, transparency-focused framework aimed at detecting and countering FIMI within its borders, both China and Russia view information as a weapon, integrate FIMI into military doctrine, and use media to reinforce state power. Despite shared goals, their approaches differ. Russia emphasizes traditional values and geopolitical influence, particularly in Europe, while China focuses on ideological control and global narrative shaping through sophisticated cognitive and technological means.

Ultimately, while Russia and China use FIMI as tools of authoritarian statecraft and global influence, the EU remains focused on defensive and values-driven strategies.

1. Introduction

Foreign Information Manipulation and Interference (FIMI) is a relatively new concept, but in being linked to disinformation and propaganda it is rooted in past actions and processes.[1] The progressively more elaborate FIMI framework has become the foundation for the EEAS to expand its focus beyond disinformation to address information manipulation on a much broader scale. This includes countering the activities of China and Russia, identified as the primary threat actors seeking to undermine EU values, procedures, and political processes. FIMI is defined as a *"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* (EEAS 2025, p. 4).

The EEAS emphasizes that for a large-scale and innovative framework to be effective, adaptable, and respectful of rights and freedoms, the 'defender community'—encompassing various actors from civil society to state institutions—must cultivate a shared understanding (EEAS 2024, p. 14). This unified, comprehensive perspective is crucial for enabling a coordinated and effective response. The FIMI concept is primarily intended to prevent harm inflicted by threat actors, with a focus on protecting democracy, procedures, and core values. As such, the FIMI framework is shaped by the EU's own priorities and threat assessments. The main risk lies in creating a rigid and ineffective system where the EU defines threats and interprets the actions of adversaries solely through its own lens.

In reality, the tactics, techniques, and procedures (TTPs) that the EU classifies under FIMI may not be viewed through a similar lens by key threat actors like Russia and China. While FIMI focuses on the manipulative behaviour of threat actors based on TTPs, Russia and China may, in contrast, define these same actions as efforts to promote truthful and "objective" narratives about their countries, aimed at combating mischaracterizations and negative perceptions. Although the EU labels these states as threat actors and views some

[1] *The paper is a deliverable of the objective of Task 2.3 of the DE-CONSPIRATOR Horizon project. Its objective is to compile evidence from archival work, to collect and put together a genealogy of concepts, and to analyse extant literature related to the strategic and military doctrines of Russia and China. The DE-CONSPIRATOR team conducted a comprehensive review of official documents, scholarly articles, reports and other relevant sources in order to trace the historical evolution of Russian and Chinese interference over time.*

of their activities in the information space as potential disruptions to democratic processes and values, Russia and China may see things quite differently. They may regard themselves as defenders rather than aggressors, framing the actions defined under the EU FIMI framework as protective measures for their regime security, moral values, and traditions against what they perceive as Western "pseudo-humanistic" and "neoliberal" ideologies.

Why is this difference in conceptualization important? Grasping the perspectives and priorities of these nations provides critical insights that can help us understand their target audience, primary objectives, and operational strategies. Without this understanding, relying solely on our indigenous definitions risks blindsiding planned efforts. This limited viewpoint could lead to false assumptions, making it harder to predict the adversary's next moves and goals, and ultimately hindering the development of an effective response.

Taking these challenges into account, this paper conducts a historical analysis of Russian and Chinese FIMI to provide insight into the key practices and factors that have shaped their approaches over time, aiding in the classification of TTPs. The paper aims to gather evidence from archives, trace the genealogy of relevant concepts, and analyse literature on the strategic and military doctrines of both nations. Official documents, reports, and scholarly sources have been reviewed to understand the historical evolution of Russian and Chinese interference, particularly in information warfare and cyber operations. This study sheds light on how Russia and China have developed their foreign interference strategies, offering insights into their objectives and tactics. By identifying patterns, the study aims to help predict future FIMI tactics and actions.

Secondly, this detailed literature research including official documents is indispensable for an improved understanding of the underlying military doctrines that underpin and provide the long term rationale for the Chinese and Russian FIMI linked activities. Ultimately the primary purpose of doctrine is to serve as the guiding framework that ensures the seamless operation of large, complex organizations like armies. It aligns the thought processes of officers, fostering a shared perspective and providing a unified foundation for action. In this context, Harald Høiback defines military doctrine as *“institutionalised beliefs about what works in war and military operations”* (Høiback 2016). Moreover, three key elements of doctrine are essential for understanding and analysing Russia's and China's FIMI strategies and activities.

The three key elements a doctrine has to contain are theory, culture and authority (Høiback 2011). Following Høiback's definition and elements of written doctrines, for a doctrine to be persuasive, it must effectively articulate the path to victory, explaining which strategies will lead to success and why they are preferable to alternatives. This clarity is essential for the doctrine to be effective. In Russia's and China's approach to FIMI, certain underlying assumptions and presuppositions that the doctrine relies on to justify itself play a crucial role at the most basic level, as reflected in the strategic documents that will be examined in this article.

Moreover, the doctrine must account for why it is suitable for the specific military force in question. It needs to consider the identity of the actor, the individuals or institutions that will implement it, and what kind of approach will be adopted towards these entities. At this stage, the cultural aspect becomes critical, as it allows us to examine how Russia and China perceive and position themselves within their doctrines. This cultural lens is important in understanding their broader strategic outlook.

Lastly, the authority dimension is necessary for validating the doctrine and ensuring its widespread acceptance by the military. Without this authoritative backing, the doctrine may struggle to gain traction. This final element underscores the real-world consequences of the strategic documents analysed in this paper, highlighting their practical impact on military operations and decision-making.

In summary, this study focuses on a thorough analysis of key strategic documents and military doctrines from Russia and China to uncover their specific methods of foreign interference. By examining these core texts, the research aims to identify recurring themes, operational patterns, and the cultural and institutional factors that shape their tactics. Understanding these elements is vital for accurately grasping the motives and strategies driving their information manipulation efforts. The importance of studying these documents lies in the insights they provide into future interference methods, which are crucial for crafting more informed and effective policy responses within the FIMI framework. Additionally, this study underlines the conceptual differences related to FIMI between the EU on the one hand and Russia and China on the other. This distinction is key to building a successful strategy for mitigating future threats. Identifying and unveiling these differences is a critical success factor to improve the effectiveness of the counter FIMI response. By the same token,

misinterpreting these divergent views could in return lead to flawed assumptions and ineffective countermeasures.

2. Information manipulation conceptualisation in the strategic and military sources of Russia

2.1. Information Manipulation According to Strategic Documents of the Russian Federation

In the context of the research of information warfare of the Russian Federation, it is essential to analyse the strategic documents developed by the Kremlin in different periods and identify the primary goals Russia sets in the information space to influence inner or outer audiences. A review of various strategic documents which were laid down during the governing period of Vladimir Putin (from 2000 to 2023) of the Russian Federation reveals Moscow's aspirations to establish itself as a dominant power in the global information space. This implies the strengthening of technological capabilities and the use of information as a weapon of powerful influence. Over the years, against the backdrop of technological progress and global political events, the tactics of using information as a weapon of influence can be seen more and more clearly in the strategic documents of the Russian Federation.

The Foreign Policy Concept of the Russian Federation (Концепция 2000), approved on June 28, 2000, consolidated the changes that had taken place in the 1990s as it was the transition to a market economy and more democratic institutions led to greater freedom of the press and an increase in media diversity, growing political activism and public discontent due to economic difficulties and perceived corruption, Economic and Political Instability, Chechen Wars and finally, an appearance a new governor - Vladimir Putin, who was emerged as a key figure in Russian politics. All these features and components proclaimed a new foreign policy course for the country in the 21st century. The introductory part of the Concept stated that among the main tasks, in addition to state security and the creation of favorable conditions for its development, were the formation of a multipolar system of international relations, a stable, fair, and democratic world order based on the generally recognized norms of international law. In addition, the discussion focused on the creation of a “belt of good neighborliness along the perimeter of Russian borders,” protecting the rights and interests of

Russian citizens and compatriots abroad, promoting a positive perception of Russia in the world, and popularizing the Russian language and culture.

According to the document, the formation of new equal, mutually beneficial partnership relations between Russia and the surrounding world has not come true. In this case, we could suppose that the “surrounding world” is mostly identified with the USA, whereas European countries, mostly the EU, are keeping the status of reliable partners. Relations with European states are a traditional priority area of Russia's foreign policy.

In this concept formally the focus was also on the protection of the interests of the individual, society, and the state. As it was mentioned, these goals have to be completed by ensuring reliable security of the country, sovereignty and territorial integrity, and strong and authoritative positions in the world community, which meet the interests of the Russian Federation as a great power as one of the influential centers of the modern world and which are necessary for the growth of its political, economic, intellectual and spiritual potential.
According to the general provision of the concept, one of the main goals in the 21st century had to be promoting a positive perception of the Russian Federation in the world and also accelerating the Russian Federation's own effective means of information influence on public opinion abroad.

In 2000, Russia still declared to take part in the formation of a “stable, fair and democratic world order based on generally recognized norms of international law, including, first of all, the goals and principles of the UN Charter, on equal and partnership relations between states.” However, at the same time, dissatisfaction is quite strictly described because of a tendency to create a unipolar world structure with the economic and power dominance of the United States growing.

For the first time, multipolarity and balance were declared as a distinctive feature of Russian foreign policy, which is explained by “Russia's geopolitical position as the largest Eurasian power.” One of the main aspects was the protection of the rights and interests of Russian citizens and compatriots abroad based on international law and current bilateral agreements.

The Foreign Policy Concept of the Russian Federation (Концепция 2008), approved on March 31, 2008, stated that the document supplements and develops the provisions of the 2000 Concept. It is noteworthy that this concept was approved following Vladimir Putin's well-known speech (Transcript 2007) at the 43rd International Security Conference in Munich in 2007. In it, he accused the United States and other Western States of undermining global security, which is regarded as a more assertive turn in Russian foreign policy.

The list of main tasks of the document included the "creation of favorable external conditions for modernization" of the country. Among the determining factors for preserving Russia's "worthy place in the world" in the document were stable economic growth, further political transformations, overcoming the resource-based orientation of the economy, and its transition to an innovative path of development.

The Concept declared the prospect of "loss by the historical West of its monopoly on globalization processes," and the activation of the policy of Western states to contain Russia was considered a reaction to this process. The main threats to international security were identified as the ignoring of the basic principles of international law by individual states, attempts to belittle the role of a sovereign state as a fundamental element of international relations, and the division of countries "into categories with different volumes of rights and obligations." For the first time, the Concept of Foreign Policy of the Russian Federation discussed Eurasian integration within the framework of the Eurasian Economic Community and the Customs Union.

The Strategy for the Development of the Information Society in the Russian Federation (Стратегия 2008) approved on February 7, 2008, focuses on transforming the Russian economy from an industrial to a knowledge-based one. The need for modern information and telecommunication technologies (ICT) is one of the main challenges in the document. In addition, it is emphasized that there is a need to reduce dependence on foreign technologies and encourage local innovations—the document aimed to position Russia among global ICT leaders by 2015.

In addition to the general goals of the strategy, several specific points are worth noting, which indicate the intention of the Russian state to increase its influence in the information space. These are:

a) “preserving the culture of the multinational people of the Russian Federation, strengthening moral and patriotic principles in the public consciousness, developing a system of cultural and humanitarian education;

b) counteracting the use of the potential of information and telecommunications technologies to threaten Russia's national interests;

c) support for the implementation of socially significant projects in the media;

d) formation of state orders for the creation and distribution of cinematographic and printed products, television and radio programs and Internet resources in the field of culture;

e) support for the activities of state and non-governmental organizations to preserve cultural and moral values, traditions of patriotism and humanism in society;

f) propaganda of cultural and moral values of the Russian people.”

As can be seen from the goals listed above and from the strategic documents of the Russian Federation in general, the Kremlin tries to present itself as being in a defensive position, facing various types of threats from the West. Accordingly, Russia's various strategic goals are framed in defensive terms, such as "protection of Russian culture" or "national interests." Hence, Russia does not see itself as a perpetrator but as a victim, forced to act to protect its own interests. Also, the positive use of the word “propaganda” is telling. States, with the exception of Marxist-Leninist regimes, generally do not use the term because of its widespread negative connotations.

The main provisions of the 2013 Foreign Policy Concept of the Russian Federation (Концепция 2013) have not undergone significant changes compared to previous documents. However, for the first time, the Concept considered the issues of using soft power in international politics, which was defined as "a comprehensive toolkit for solving foreign policy problems based on the capabilities of civil society, information, and communication, humanitarian and other methods and technologies alternative to classical diplomacy." The most recent concept released in 2023 (Концепция 2023), in contrast, makes to reference to soft power whatsoever, yet speaks of the hostile information environment to overcome.

The Concept stated that in the new system of international relations, which was affected by the global financial and economic crisis, the West was losing its dominant role in both politics and economics. The potential for power and development was shifting to the East, primarily to the Asia-Pacific region. The risks of the destructive use of "soft power" and human rights concepts for the purpose of political pressure on sovereign states and interference in their internal affairs were noted. Attempts to regulate crises by using unilateral sanctions, pressure, and other forceful measures outside the UN Security Council were named as one of the threats to international security. The document, also for the first time, specifically spoke about the need to facilitate Ukraine's involvement in deep integration processes.

The Concept of the Russian Federation's State Policy in the Area of International Development Assistance (Концепция 2014) outlines Russia's strategic approach to providing international aid. The strategy's significant goals include “strengthening a positive image of the Russian Federation and its cultural and humanitarian influence in the world; facilitating integration processes in the space of the Commonwealth of Independent States and improving the quality of education, especially primary and vocational training, as well as their availability for the population in the recipient States.”[2]

The Military Doctrine of the Russian Federation (Военная 2014) outlines the country's strategic approach to national defence and security. Despite a reduced likelihood of large-scale war, Russia perceives growing military dangers, particularly in the information sphere and within its borders. Key external threats, according to the doctrine, include NATO enlargement, destabilization in neighboring regions, deployment of foreign military forces near Russia, and the development of strategic weapons systems. The document also highlights concerns about terrorism, extremism, and the use of information technology for military and political purposes.

Furthermore, Russia identifies one of the primary internal threats as “activities aimed at influencing the population through information, particularly targeting the country's youth, with

[2] *Authors' note: The document speaks of the regions of Georgia occupied by the Russian Federation that are not recognized by the international community as independent states.*

the intent to undermine historical, spiritual, and patriotic traditions related to defending the Fatherland."

The military doctrine also provides a detailed description of the characteristics of modern military conflicts. It emphasizes, among other means, the comprehensive use of military force alongside political, economic, informational, and other non-military measures. It states that these actions are implemented through the extensive use of the population's protest potential, the employment of indirect and asymmetric methods of action, and the utilization of externally financed and controlled political forces and social movements.

To address the described threats, the document outlines several strategic measures. In the realm of information space, it includes creating conditions that reduce the risk of using information and communication technologies for military-political purposes, developing forces and means of information warfare, and fostering dialogue with interested states on national approaches to countering military dangers and threats arising from the large-scale use of information and communication technologies for military-political purposes. These topics are not new in this particular document, as they were also outlined in past military doctrines. However, with the development of information technologies, they are emphasized more than they were in the documents from the 1990s and 2000s.

The Foreign Policy Concept of the Russian Federation (Указ 2016), approved by presidential decree on November 30, 2016, included two new foreign policy objectives, which fall under the information realm: strengthening Russia's position as one of the influential centers of the modern world and strengthening the position of Russian media and mass communications in the global information space.

The Concept noted a serious crisis (this concept was updated after 2014 when the European Union (archived content, since 2014) and the United States (U.S. Department of State, 2014) imposed sanctions on Russia due to the annexation of Crimea) in relations between Russia and Western countries caused by the geopolitical expansion of the United States, NATO, and the European Union. The document noted that while maintaining an interest in constructive cooperation with the United States, Russia "does not recognize the extraterritorial exercise of its jurisdiction by the United States outside the framework of international law, does not

accept attempts to exert military, political, economic or other pressure, and reserves the right to respond harshly to unfriendly actions."

The Doctrine of Information Security of the Russian Federation (Доктрина 2016), approved by a presidential decree in December 2016, outlines Russia's official stance on safeguarding national security within the information sphere. According to the document, the information security system of the Russian Federation includes: owners of critical information objects and organizations operating such objects; mass media and mass communications; monetary, foreign currency, banking and other financial institutions; telecommunication operators; information system operators and other actors related to the information security field. As the document broadly defines this sphere, it also emphasizes the protection of national interests, sovereignty, and stability against internal and external threats. The doctrine identifies critical dangers such as foreign intelligence activities, information warfare, and extremist groups' misuse of information technologies. It also highlights challenges like the dependency on foreign technology and the need for competitive domestic alternatives. The doctrine draws strategic objectives, including enhancing military and state information security, protecting critical infrastructure, and promoting Russian interests in international information security systems.

The doctrine repeatedly emphasizes that “concrete States” use informational and psychological mechanisms to influence regions across the world, undermining sovereignty and violating the territorial integrity of other states. Additionally, the document notes that „there is a trend among foreign media to publish an increasing number of materials containing biased assessments of State policy of the Russian Federation. Russian mass media often face blatant discrimination abroad, and Russian journalists are prevented from performing their professional duties. There is a growing information pressure on the population of Russia, primarily on the Russian youth, with the aim to erode Russian traditional spiritual and moral values”.

In response to this challenge, it is noted that it is important to „provide the Russian and international community with reliable information on the State policy of the Russian Federation and its official position on socially significant events in Russia and in the world, and apply information technologies to ensure the national security of the Russian Federation

in the sphere of culture.“ Furthermore, the doctrine declares the Russian Federation's national interests in the information sphere, which, among other things, include “applying information technologies for the preservation of cultural, historical, spiritual and moral values of the multi-ethnic people of the Russian Federation.”

The Russian Federation's National Security Strategy (July 2, 2021) (Стратегия 2021) focuses on strengthening defence capabilities, internal unity, political stability, and economic modernization to ensure sovereignty and resist external pressures. According to the document, the implementation of the aforementioned policy goals is necessary for Russia to become one of the influential centers of global politics. At the same time, the strategy states that efforts of various states to isolate Russia, along with the double standards they employ, hinder the enhancement of multilateral effectiveness in areas important to the international community, including Europe.

The document also highlights that the “problem of moral leadership and the creation of an attractive ideological basis for the future world order is becoming increasingly urgent. Against the backdrop of the crisis of the Western liberal model, a number of states are making attempts to deliberately erode traditional values, distort world history, revise views on the role and place of Russia in it, rehabilitate fascism, and incite interethnic and interfaith conflicts. Information campaigns are being conducted aimed at creating a hostile image of Russia. The use of the Russian language is being restricted, the activities of Russian mass media and the use of Russian information resources are being banned, and sanctions are being introduced against Russian athletes…”

The strategy declares that unfriendly countries are exploiting Russia's socio-economic issues to disrupt its unity, radicalize protests, inspire “color revolutions,” and create instability. It also suggests that to destabilize Russia's socio-political situation, false information is spread, and the internet hosts content from extremist groups, promoting riots, illegal activities, suicide, criminal behaviour, and drug use, and these harmful influences mainly target young people. Additionally, as the strategy claims, transnational corporations seek to monopolize the Internet and control information by imposing censorship and blocking alternative platforms.

The strategy outlines Russia’s national interests and priorities regarding information security. One of the critical goals in this regard is to develop a safe information space and protect

Russian society from “destructive information and psychological influence,” as well as “protect traditional Russian spiritual and moral values, culture, and historical memory.” “Protection of national interests and citizens of the Russian Federation outside its territory” is also declared as one of the main priorities.

Article 57 of the National Security Strategy outlines the objectives for ensuring information security. Several of these tasks are particularly notable in the context of Russian information influence. These are the “development of forces and means of information warfare; dissemination to the Russian and international public of reliable information about the domestic and foreign policies of the Russian Federation.” A separate chapter in the document is dedicated to „Protection of Traditional Russian Spiritual and Moral Values, culture and Historical Memory.” This chapter discusses various threats against “basic moral and cultural norms, religious foundations, the institution of marriage, and family values” and states that: “Traditional Russian spiritual, moral, and cultural-historical values are subject to active attacks by the United States and its allies, as well as by transnational corporations, foreign non-profit, non-governmental, religious, extremist, and terrorist organizations…”

According to the strategic document, the protection of traditional Russian spiritual and moral values can be achieved by the following measures: “protection of historical truth”; “popularization of the achievements of Russian science and technology, literature, artistic culture, music and sports, including through the revision of the curricula of educational organizations”; “support for religious organizations of traditional faiths, ensuring their participation in activities aimed at preserving traditional Russian spiritual and moral values, harmonizing Russian society, spreading the culture of interfaith dialogue, and countering extremism”; “formation of a state order for conducting scientific research, publishing popular science materials, creating works of literature and art, cinematographic, theatrical, television, video and Internet products, providing services aimed at preserving traditional Russian spiritual and moral values and culture, protecting historical truth and preserving historical memory, as well as ensuring quality control of the implementation of this state order…”

The Russian National Security Strategy assigns a special role to deepening the country’s international relations with its friendly countries and aims to increase Russia's global role in

humanitarian, cultural, scientific, and educational fields. In addition, it aims to strengthen the Russian language's position as the language of international communication.

Besides the above-mentioned, within the international context, the following information-related issues can be distinguished from the strategy's objectives: “providing support to compatriots living abroad in the exercise of their rights, including the right to preserve the all-Russian cultural identity, ensuring the protection of their interests”; “strengthening fraternal ties between the Russian, Belarusian and Ukrainian peoples”; “strengthening the position of Russian mass media and mass communications in the global information space”; “development of international cooperation in the interests of creating a safe and equal global information space.” This passage depicts a seamless transition from information operations within Russia for regime/national security to FIMI [because these operations would occur abroad], thanks to two drivers: an aspiration to “extraterritorial jurisdiction” over Russian diaspora and a soft conception/denial of Ukrainian sovereignty.
The Concept of the Foreign Policy of the Russian Federation (Концепция в2023), approved on March 31, 2023, declares “Russia’s special position as a unique country-civilization and a vast Eurasian and Euro-Pacific power that brings together the Russian people and other peoples belonging to the cultural and civilizational community of the Russian world.”

In terms of informational strategies, the concept sets key strategic goals and tasks to promote Russian foreign policy interests. Those are as follows: “to develop safe information space, to protect Russian society against destructive informational and psychological influence”; “to ensure that Russia is perceived abroad objectively, consolidate its position in the international information space”; “to enhance Russia's role in the global humanitarian space, consolidate the position of the Russian language in the world, and contribute to the preservation abroad of historical truth and the memory of Russia's role in world history”; “to protect abroad, in a comprehensive and effective way, the rights, freedoms and legitimate interests of Russian citizens and entities”; “consolidate international efforts to ensure respect for and protection of universal and traditional spiritual and moral values (including ethical norms common to all world religions), and counter the attempts to impose pseudo-humanistic or other neo-liberal ideological views, leading to the loss by the humankind of traditional spiritual and moral values and integrity.” The conceptualisation of “information space” in the Russian strategic thinking can be found in the Doctrine of Information Security of the Russian Federation,

approved in 2016. It defines the information space as a combination of information, informatization objects, information systems and websites within the information and telecommunications network of the Internet (hereinafter referred to as the "Internet"), communications networks, information technologies, entities involved in generating and processing information, developing and using the above technologies, and ensuring information security, as well as a set of mechanisms regulating public relations in the sphere.

Furthermore, the concept outlines that it is necessary to form an “objective perception of Russia abroad, strengthening its position in the global information space, countering the coordinated anti-Russian propaganda campaign carried out on a systematic basis by unfriendly states and involving disinformation, defamation and incitement to hatred, and ensuring free access of the population of foreign states to accurate information, the Russian Federation intends to give priority to:

1) making truthful information about the Russian Federation's foreign and domestic policies, its history and achievements in various spheres of life, and other accurate information about Russia available to the widest possible foreign audience;

2) facilitating the dissemination of information abroad to promote international peace and understanding, develop and establish friendly relations between states, strengthen traditional spiritual and moral values as a unifying principle for all mankind, and enhance Russia's role in the global humanitarian space;

3) ensuring protection from discrimination abroad and assisting in strengthening the position of Russian information and communications media, including domestic digital information platforms, in the global information space, as well as constructively-minded media of compatriots living abroad towards Russia;

4) improving the tools and methods of information support for the foreign policy activities of the Russian Federation, including more effective use of modern information and communication technologies, including social networks;

5) improving international mechanisms and norms of regulation and protection of information and communication media, for ensuring free access to them and creating and disseminating information…”

The strategy does not mention Ukraine, and the invasion of this country is called “measures to protect vital interests in the ukrainian [with lowercase] direction”. Of course, using the

terminology “ukrainian” is not meaningless. This is the part of the narrative “substantiating” that Ukraine is part of Russian territory. Several times, Vladimir Putin has tried to prove that using etymological aspects of the word “Ukraine” (U Kraia - in Russian У края - has a meaning “next to the state/country”, or “by the border”/”borderland”) in different interviews. The last one was with Tucker Carlson (Герейханова 2024).

The concept of 2023 also noted that strategic security has been undermined, and the risks of clashes between major states (including nuclear powers) are increasing. Western countries, the Concept emphasizes, have “unleashed a new type of hybrid war against Russia. At the same time, Russia does not consider itself an enemy of the West, does not isolate itself from it, does not have hostile intentions towards it, and expects that in the future, Western countries will return to pragmatic interaction with Russia based on respect for each other's interests.” Hence, Russia does not perceive itself as a perpetrator but as a victim (Aischmann 2023).

Besides the official state documents, an article published in January 2013 by Valery Gerasimov, now the Chief of the General Staff of the Armed Forces of the Russian Federation, Colonel General, is also worth mentioning as it forms part of the official approach. This article outlines the evolving nature of warfare in the 21st century, where the boundaries between war and peace are increasingly blurred. He argues that modern conflicts often involve a mix of traditional military actions and nonmilitary means, such as political, economic, and informational strategies.

As Gerasimov stresses: “The information space opens wide asymmetrical possibilities for reducing the fighting potential of the enemy… Among such actions are the use of special operations forces and internal opposition to create a permanently operating front through the entire territory of the enemy state, as well as informational actions, devices, and means that are constantly being perfected… We must not copy foreign experience and chase after leading countries, but we must outstrip them and occupy leading positions ourselves” (Gerasimov 2013).

The tactics outlined in the article are also reflected in the Russian Federation's modern strategic documents. The main goals and strategy lines of the documents reviewed in this

document are transformed into practical activities, as Pomeranstev and Weiss (2014) argue: “The Kremlin exploits the idea of freedom of information to inject disinformation into society. The effect is not to persuade (as in classic public diplomacy) or earn credibility but to sow confusion via conspiracy theories and proliferate falsehoods”.

2.2. Information Manipulation According to Russian Pro-governmental Academics

This part of the paper will discuss the Russian pro-governmental academic views on information manipulation. While there are still remnants of independent social sciences in Russia after the beginning of the full-scale invasion, the majority of scientists are constrained by (self-)-censorship, due to the existence of laws that are aimed at reducing the amount of available information. Ironically, one of these laws is supposed to target “fake” information and was initially used during the COVID-19 pandemic to curb the spread of false information about the disease (Sherstoboyeva 2024). In the context of the full-scale invasion, the freedom of speech has shrunk even more significantly (OVD-info 2024) and, for instance, several international peer-reviewed journals (e.g., Russian Journal of Communication) have ceased their publications. Thus, the majority of articles and books available hardly offer a critical outlook on governmental policy. This part of the paper specifically focuses on academic articles and books that were published by academic institutions and/or academics affiliated with the Russian army and Russian state institutions. Usually not contradicting the official documents, such as the Foreign Policy Concept or National Security Strategy, these papers go into more detail about the issues that are mentioned in the official documents, often using much more aggressive language than the government. The “usual suspects” are journals like “Army Collection”, “Bulletin of Military Education”, “Military Thought” or “Military History Journal”.

The Russian academic circles treat information manipulation as a phenomenon that is targeted at Russia and to which the Russian government should adequately respond. Some

of the scholars display a superficial knowledge of the Western media literature (e.g., two-step flow communication, CNN effect) and are convinced that most of the international scandals involving Russia (e.g., Panama Papers or WADA scandal) were acts of informational-psychological warfare on behalf of the West. Additionally, there is a deep-seated assumption among the quoted "scholars" that what they call "the collective West" is trying to undermine the Russian state by injecting information that they see as "harmful" to the stability of Russian society. These "scholars" have developed playbooks and guides that reflect their assumptions about Western propaganda and are geared towards provoking an emotional response from the audience.

Russian military analysts are convinced that the Third World War will be an informational-psychological one (Samokhvalova 2011; Vladimirov 2013; Markov 2018; Kiselev 2015). According to Manoilo (2003), "Information and psychological warfare is currently considered by most of the world's leading countries as an effective and universal means of achieving foreign policy goals" (p. 22). Russian Military Doctrine has officially emphasized the need to develop armed forces and means for an "information confrontation" at least since 2010 (Kremlin 2010), even though some type of information manipulation has been present both in Soviet and American foreign policy strategies since the Cold War (Cull 2009) and in Russian academia informational -psychological security defined as a problem in 1996 (Smolyan et al. 1996). In the context of Russia's war against Ukraine, some "scholars" even lament the absence of study programs aimed at training information security specialists and disinformation experts (who are able to "manipulate the meanings"), inadvertently admitting the popularity of disinformation studies in the West (Makashova 2023).

The Russian military and political elite's belief in the plots against the Russian state is rooted in various conspiracy theories that argue that "the West" is on a quest to destabilize Russia through corrupting Russian core values and its society (Gaufman 2017; Yablokov 2018, Radnitz 2022). For instance, one of the main threats related to information security is the "falsification of history" (Filonenko et al 2024) in order to "invade the value-sense sphere of a target audience" and ultimately to "organize mass dissatisfaction among the population", with

the United States specifically perpetrating a “civilizational containment” through “mental wars” (Zarudnitsky 2023). The United States Defense Intelligence Agency’s report on Russian Military Power discusses how “Information Confrontation” is “strategically decisive and critically important to control its domestic populace and influence adversary states," encompassing “Informational-Technical” (defence, attack, and exploitation) and “Informational-Psychological” (changing people’s behaviour or beliefs in line with Russian government’s agenda) strategies. At the same time, Russian military scholars consider the whole notion of “hybrid warfare” as a part of a “russophobic discourse” that showcases how Western academia has become its propaganda arm (Il'ichev 2023).

Vladimir Lepsky, professor of Diplomatic Academy in Moscow argues that the “informational-psychological security” has become increasingly important due to “information expansion from a number of developed countries, carrying out global information and propaganda activities in order to spread the worldview, political and spiritual values and ideals of the Western world” (Lepsky 2002). This is supposed to be carried primarily through mass media. Here is the list that of the presumed TTPs compiled by Andrey Manoylo (2003), professor at the Moscow State University and Founder and President of the Association of Information Operations Specialists (founded in 2019):

1. Manipulation of true information.
2. Biased selection of topics and materials.
3. Distribution of airtime disproportionate to the true meaning of information fragments.
4. Fragmentary presentation of information.
5. Intentionally equalized presentation of poorly comparable factors - the technology of "media amplification".
6. Distraction of the audience's attention from a truly significant, but politically unfavourable event for coverage by poor-quality presentation of information material.
7. Selection of an advantageous moment for informing the population (for example, for the release of compromising materials).

8. Emotional commentary, presentation of what is happening.
9. Two-stage communication flow: use in comments of the opinions of competent persons respected by society.
10. Using charming and attractive people as TV presenters, who are most persuasive in cases where subjective preference plays a major role.
11. A certain sequence of providing information: when expressing contradictory points of view, the most persuasive information is the one conveyed first.
12. The art of specialized editing of information (for example, combining in time a tendentious soundtrack and documentary video).
13. Bringing information only to a certain group of the population (for example, by territorial, national, religious or social characteristics); this technique helps to identify and form groups of like-minded people.
14. Broadcasting video information obtained using the capabilities of computer graphics, and/or artificially synthesized speech, for example, government, public figures.
15. The technology of influencing the media to deform archetypal images, introducing elements of instability, disorganization, chaos, uncertainty and fear into public consciousness.
16. Using the media as a channel for delivering targeted disinformation to the population and the country's leadership.
17. Technologies of manipulating public opinion polls in the media.
18. Using the media as a tool for directly delivering threats, ultimatums, "impulses" of dictate and intimidation to society and individuals.
19. "The CNN effect": the concept that global, real-time media affects diplomacy and foreign policy (Livingston 1997).
20. Demonstrating the superiority of one's culture (civilization) in propaganda materials is the most important substantive element of informational and psychological influence for the media of leading Western countries (including NATO).

21. Exploitation of all kinds of rumours in the media that can purposefully influence the information and psychological climate in society.
22. Use of the media as a tool for directly communicating threats, ultimatums, "impulses" of dictatorship and intimidation to society and individuals.
23. Technology of "reflexive control".

While some of these TTPs are outdated (e.g., CNN effect), others still seem quite relevant and practical for the information manipulation strategies employed by the IRA. Moreover, in the vast majority of the "academic" texts on information manipulation, the main actor is considered the West and specifically NATO countries. China, for instance, is barely mentioned as an actor in global information war, unless it's a reference to Sun Tzu (Smirnov 2013). Manoylo also wrote a "practical guide" for information manipulation (2018), where he analysed what he perceived as information-psychological war instances against Russia (attempted murder of Skripals, Panama papers etc). According to him, "the West" has changed its strategy in information-psychological war after the annexation of Crimea (which he views as a pivotal moment in Russia-West relations) and has started using a specific "playbook" of strategically leaking information and using "investigative journalists". According to Manoilo, a Russian "operation" is supposed to follow the following structure: "provocation (1); bait (2); exposure (3); inoculation (4)", where the main purpose is to provoke an emotional response from the victim.

This "academic" view has been partially corroborated by the documents obtained by The Insider, who have managed to access the documents from the Russian External Intelligence Service (SVR). The most relevant TTPs are quoted below with my emphasis:

1. "The reliance on the **'old' media**; commitment to those forms of information and propaganda work that have demonstrated **near-zero** efficiency for not years, but decades; an attempt to continue foreign broadcasts by RT and Sputnik; even the relatively 'fresh' trend of supporting loyal Telegram channels - all of this, individually and together, does not justify the expectations placed on the performers and demiurges. The lack of creativity, hypocrisy and moralizing aggravate the current situation."

2. “In order to **deepen internal contradictions** between the ruling elites, **stimulate protest activity** of opposition forces, escalate anti-government demonstrations and **“stir up”** the amorphous part of the electorate in the main enemy countries by means of a controlled non-governmental organization (for reasons of conspiracy and security), whose competence will include the implementation of secret influence actions on authoritative representatives of the above-mentioned circles”.
3. The proposed option for conducting information warfare allows for the possibility of using non-standard methods of influence that are not included in the toolkit of the Federal Information Warfare Institution. Due to the frequency, obsession, aggressive form, and incorrect presentation, we should expect a negative reaction from the target audience in fulfilment of the aforementioned goals.
4. "**Appealing not to reason, but to emotions**, namely to the irrational component of human sensory-psychological perception, contributes to the fastest and most reliable achievement of the goals set before the propaganda machine. Taking into account the above, it seems appropriate to consider the issue of shifting the vector of the main efforts in information and propaganda work against the states of the main enemy to the transmission of the so-called **negative agenda**.
5. "At the same time, we could organize effective counteraction to the collective West, and specifically in their field, using the methods and techniques they have developed on the Internet platforms they control. The leitmotif of our cognitive campaign in the main enemy countries is proposed to be the awakening of the strongest emotion of the human psyche in recipients - **fear**. It is fear for the future, **uncertainty** about tomorrow, the inability to make plans for the future, the uncertainty of the fate of children and future generations, the cultivation of the listed triggers that overwhelm the subconscious of an individual with panic and horror. The infliction of successive cognitive blows on Central Asia, linked by a single plan, will first of all form a stable rejection of the political course of

governments and supranational institutions of the EU, and in the long term will lead to an **escalation of protest activity and other negative consequences**."

6. By using special social engineering tools, we will encourage a significant portion of the target audience (regardless of their social status) to **switch to the main resources** under our control, study additional materials, show interest in them, and distribute them among their immediate circle. In the long term, we will be able to establish stable business relationships with particularly active "retransmitters," thereby transferring them to the category of **public opinion leaders** (POL) and encouraging them to expand their own, and therefore our, audience quantitatively and qualitatively."
7. "An approximate scheme of information impact looks like this: we take as a basis a website created for an **"information agency"** (or an "independent investigation agency"). All materials intended for inspiration will be accumulated on this website. In addition, the printed form will be duplicated by **audio and video on popular video hosting sites** (YouTube, RuTube, etc.). To enhance the effect, we **cut the main video into shorts** and **publish it 1-2 times a day.** Links to the content are introduced into the target audience's electronic communication media using a **unique algorithm** based on the new module of the "Storm" platform and special software. In addition, we simultaneously launch **campaigns on social networks**, supplementing them with **targeted mailings via messengers** in accordance with the recipient geolocation plan."
8. "The appropriate and effective number of demonstrators is up to 100 people. More is pointless and carries political risks. Less is of little resonance and ineffective. The cost of a demonstrator going to the action is 100 euros. The action lasts for 1 hour. During this time, photo and video shooting is carried out for subsequent distribution in the media."

3. Information Manipulation Conceptualisation in the Strategic and Military Doctrines of the People's Republic of China

3.1. Information Manipulation Concepts of the Chinese Communist Party

It makes sense to distinguish between FIMI operations of the Chinese Communist Party (CCP) and those of the People's Liberation Army (PLA) (even if the PLA has to be considered as the military arm of the CCP), because they operate on different levels. While the Party's influence operations are primarily at the strategic level, the military's activities span both the strategic and operational levels (Yamaguchi et al. 2023, p. iii).

For China, the battle for information and influence is essentially fundamentally driven by concerns over regime security. The Party has been long concerned that foreign information could undermine its control over the domestic population, often referred to in terms like "ideological security" (意识形态安全; see Tang 2019), "cultural security" (文化安全) or more recently, "cognitive security" (认知安全). The influence of events such as the Arab Spring, which saw the use of social media in the overthrow of authoritarian regimes, has only heightened these concerns. Beijing's objective is not only to correct Western "misperceptions" but also to proactively promote the Chinese perspective and narrative both domestically and internationally. By advancing the Chinese narrative in global and domestic discourse, China believes that it can counter what it perceives as Western efforts to infiltrate the fabric of its society by spreading universal values such as human rights and democracy (PRC Central People's Government 2016). In the view of the party, expanding domestic and international influence and maintaining domestic stability are directly interlinked. Thus, any activities that are regarded as Chinese FIMI in the West are conceptualized domestically as

defence against Western interference and attempts to destabilize the Party's governing and thus by extension China.

The key concept in the Party's ideological battle is **"discourse power"** (话语权), which literally translates as the "right to speak" or the "power to speak", and implies the power to create discourse and make it internationally accepted. The topic is frequently raised by Xi Jinping and high-ranking party cadres. Discussions about how to increase China's international discourse power vis-a-vis the West are abound in theoretical party journals like *Qiushi*, in the opinion pages of the party newspaper *People's Daily* (人民日报) or in the PLA newspaper *PLA Daily* (解放军报). A core reference document on that is a speech given by Xi Jinping at the National Propaganda and Ideology Work Conference (全国宣传思想工作会议) in Beijing on 19 August 2013, at which he stressed that

> *Efforts should be made to enhance international communication capabilities, innovate the methods of external propaganda, strengthen the construction of a discourse system, endeavour to create new concepts, categories and expressions that integrate China and the rest of the world, tell China's stories well, make China's voice heard, and enhance China's influence in the international discourse.*
> 要着力推进国际传播能力建设，创新对外宣传方式，加强话语体系建设，着力打造融通中外的新概念新范畴新表述，讲好中国故事，传播好中国声音，增强在国际上的话语权。(Xinhua 2013).

Xi's expression "telling China's stories well and making China's voice heard" (讲好中国故，传播好中国声音) is referenced widely throughout party literature; in 2021 *Qiushi* published an

article listing related quotes from Xi's speeches, thus offering kind of a reference guide to party members to quote Xi correctly (Qiushi 2021).

Main means to increase international discourse power are external propaganda work, now officially termed as **"international communication work"** (国际传播工作) and "**United Front work"** (统一战线工作):

External propaganda (对外宣传) work:

- primary objectives can be summarized as to tell China's narrative to the world and publicize Chinese government opinions and Chinese culture; to counter foreign propaganda; to counter Taiwan independence movements and activities by their supporters; and to propagate China's foreign policy (Yamaguchi et al., 2023, p. 31)
- tools: increasing the presence of state media, disseminating official views through foreign media, cultivating foreign media outlets that are friendly to China, purchasing foreign media outlets, and engaging in social media campaigns and activities led by diplomats. Notably, exploiting foreign media to deliver Chinese propaganda is termed as **"borrowing a boat out to sea"** (借船出海) (Cao 2020).
- While the traditional term for external propaganda is the literal translation 外宣, the currently dominant term/concept is "international communication" (国际传播), specifically "international communication work" (国际传播工作) and "international communication capability" (国际传播能力). The Chinese leadership clearly believes that the capabilities are insufficient. At a politburo meeting on 31 May 2021, Xi stressed the need "to strengthen and improve international communication work" (加强和改进国际传播工作) (Xinhua 2021).

United Front Work (统一战线工作): a strategy of countering a major adversary by creating internal rifts in the major adversary and gaining friendly allies. “Regulations on the Work of the Unified Front” (中国共产党统一战线工作条例) issued in 2021 define in Chapter 10 overseas united front work, including “to curb separatist forces such as "Taiwan independence" and safeguard the core interests of the country” and “create a favorable international environment.” (CCPCC 2021). There are 12 categories of united front work targets: members of minor parties (parties other than the CCP which are permitted to exist); people with no party affiliation; non-Party intellectuals; ethnic minorities; religious figures; members of the non-public ownership economy (private economy); members of new social strata; overseas and returned overseas students; compatriots in Hong Kong and Macao; compatriots in Taiwan and their relatives in the mainland; overseas Chinese, returned overseas Chinese, and relatives of overseas Chinese; and others who need to be liaised with. Many of the categories concern national integration in China. On the other hand, overseas Chinese and overseas Chinese students have direct overseas associations, and ethnic minorities and religious figures are not confined to China. In addition, united front work with private entrepreneurs and members of new social strata will have impacts overseas in line with the global development of the Chinese economy. Taiwan’s unification with the mainland is also a long-time wish of China, and the united front will be critical to bringing Taiwan closer to the country. The relevance of United Front work has been

reiterated by Xi in a speech at the Central United Front Work Conference (中央统战工作会议) on 29 July 2022, the speech was published in *Quishi* in spring 2024 (Xi 2024).

Main organizations/groups behind Party State information activities:

- Central Leading Group on the United Front Work (中央统一战线工作领导小组), established in 2015, headed by Wang Yang
- Central Leading Group for Propaganda and Ideology (中央宣传思想领导小组): headed by Wang Huning, provides overall guidance and coordinates propaganda work
- Central Military Commission (中央军事委员会), specifically the Political Work Department of the CCP Central Military that supplanted the General Political Department. following the mid-2010s PLA reform
- Central Cyberspace Affairs Commission (中央网信委) is at the top of the organizations responsible for cybersecurity of the entire Party-state.
- Central Propaganda Department (中共中央宣传部): influential in day-to-day operations.

3.2. Information Manipulation Concepts of the People's Liberation Army

PLA offers no publicly available "doctrines" in the Western sense, therefore, when it comes to internal hierarchy and the approaches, the sources are scarcely available and subject to interpretation. As the armed wing of the CCP in an era of informationised operations [信息化作战], the PLA is in the business of using information to influence foreign perceptions and behaviours against a variety of foreign entities, such as enemy military and political forces and neutral or allied third parties (Harold et al. 2021).

Three Warfares (三种战法)

The PLA's engagement with information warfare can be traced back to its traditional practices of political work and external propaganda, which were primarily aimed at communicating Chinese messages to foreign audiences and undermining enemy morale. Over time, particularly after the 2003 U.S. invasion of Iraq, the PLA came to believe that that modern warfare is defined by information and is thus described as “informationized warfare” (信息化战争). Till the mid-2000s, the PLA developed the concept of "Three Warfares" (三种战法), which includes "psychological warfare" (心理战), "public opinion warfare" (舆论战), and "legal warfare" (法律战). The “Three Warfares” were mentioned and outlined in several strategic texts. The PLA Political Work Regulations (整治工作条列) (2003, 2010, 2021) name them as part of wartime political work. In 2005, the Central Military Commission (CMC) ratified guidelines (刚要) for “public opinion warfare”, “psychological warfare”, and “legal warfare”, officially incorporating the concepts into the PLA’s education, training, and preparation for military struggle. While the guidelines are not publicly available, their content is authoritative described in open-source PLA literature (Wu and Liu 2014). Textbooks used in education for officers illustrate the role of the “Three Warfares” in PLA strategic thinking:

- *Science of Military Strategy* (SMS, 战略学), 2020 (earlier editions 2017 and 2015) by National Defense University, and 2013 by PLA Academy of Military Science:

- The 2013 version of SMS introduced introduced the concept of huayuquan (话语权) through the use of information, belief, and mentality (信息一信仰一心智) (Kania 2016: 11).

- The 2015 NDU SMS provides an overview of "public opinion warfare", "psychological warfare," and "legal warfare" and guidance regarding their implementation. According to the text, public opinion warfare involves using public opinion as a weapon by propagandizing through various forms of media in order to weaken the adversary's "will to fight" (战斗意志), while ensuring strength of will and unity among civilian and military views on one's own side. "Psychological warfare" seeks to undermine an adversary's combat power, resolve, and decision-making, while exacerbating internal disputes to cause the enemy to divide into factions (阵营). "Legal warfare" envisions use of all aspects of the law, including national law, international law, and the laws of war, in order to secure seizing "legal principle superiority" (法理优势) and delegitimize an adversary. Each of the "Three Warfares" operates in the perceptual domain (认知领域) and relies upon information for its efficacy. For "public opinion warfare", the requirements outlined are to "demoralize one's opponent by a show of strength" (先声夺人), "create momentum to control the situation" (造势控局), "assail strategic points" (抨击要害), and "seek the avoidance of injury" (趋利 避害). In particular, it is critical to be the first to release information in a contingency and actively guide public opinion in order to achieve and preserve the initiative on the "public opinion battlefield".

Beyond efforts to exploit an adversary's shortcomings, the opponent's attempts to engage in "public opinion warfare" must also be countered. According to Kania (Kania 2016: 12), this approach is reflected in Beijing's attempts to influence domestic and international public opinion with regard to the U.S. role in Asia—including claiming that the U.S. is at fault for regional tensions and the "militarization" of maritime territorial disputes, while frequently denouncing U.S. "hegemony" and pursuit of "absolute security." The implementation of "legal warfare", which seeks to provide legal support to operational success, is in-formed by the principles to "protect national interests as the highest standard" (以维护国家利益为最高准 则), "respect the basic principles of the law" (尊重法律的基本准则), "carry out [legal warfare] that centers upon military operations" (围绕军事行动展开), and "seize standards [and] flexibly use [them]" (把 握规范灵活运用). This approach emphasizes the necessity of a nuanced understanding of relevant domestic and international law in order to engage in "legal struggle" and achieve the initiative. In the context of the South China Sea dispute, this has involved the utilization of rather tortuous interpretations of international law to oppose the Philippines' position and seek to delegitimize the arbitration process. (Kania 2016: 12-13)

- The 2020 SMS version has a new addition that China "must unwaveringly uphold the strategic thought of 'active defense'" as it is beneficial for China to "seize the moral high ground" and "gain political and diplomatic advantages." (Xiao 2020: 31 quoted in Clay and Lee 2022). "Active defense" has been China's military strategy since 1949, heavily influenced by Maoist guerilla warfare legacies, emphasizing

the strategy of luring the enemy deep into China's territory before transitioning to a counterattack with numerically superior forces – a philosophy that was development primarily with a potential U.S. or later Soviet invasion of China in mind (Fravel 2019: 62-63). After the U.S. special troops defeated the Iraqi military in the Gulf War, China shifted the strategy to a focus on fighting local wars under high-technology conditions along China's periphery, highlighting a quality-over-quantity force (Tosi 2023: 90). Under Xi Jinping, the focus shifted to joint operations between PLA and PLAN to enable joint military operations capable of fighting outside of the Chinese mainland and its immediate strategic periphery, namely Taiwan and the South China Sea (Tosi 2023: 94).

· *An Introduction to Public Opinion Warfare, Psychological Warfare, [and] Legal Warfare* (舆论战心理战法律战概论), by Wu Jieming (吴杰明) and Liu Zhifu (刘志富), National Defense University Press, 2014:

The text presents a comprehensive overview of the "Three Warfares", including their primary missions, historical development, theoretical foundation, basic principles, implementation, and tactics. The text illustrates the NDU's sustained efforts to develop a "science of the Three Warfares" ("三战"学). This is informed by the study of variety of traditional, ideological, and contemporary precedents, from the ancient Chinese emphasis on the use of "stratagems" (谋略) to the U.S. military's perceived engagement in analogous practices. At a basic level, the primary purpose of the "Three Warfares" is to influence and target the adversary's psychology through the utilization of particular information and the media as "weapons". In particular, the "Three Warfares" are seen as critical to increasing the PLA's "soft power" (软实力) and contributing to its success in future wars (see Kania: 11). As relevant functions of the "Three Warfares", the textbook

lists: control of public opinion (舆论控制), blunting an adversary's determination (意志 挫伤), transformation of emotion (情感转化), psychological guidance (心智诱导), collapse of (an adversary's) organization (组织瓦解), psychological defence (心理防御), and restriction through law (法律制约). According to the text, the implementation of the "Three Warfares" should be, i.a. integrated with the national political and diplomatic struggle.

Cognitive Domain Operations (认知域作战)

Since the late 2010s, there has been a notable shift in the PLA's focus towards "cognitive domain operations" (CDO) (认知域作战), a concept that has become the primary framework for cyber-enabled influence operations (Beauchamp-Mustafaga 2023). CDO appears to be to be intended as a technologically driven update to bring the "Three Warfares" concept – developed in the information-driven era of informatization (信息化) – into the new AI-driven era of intelligentization (智能化) (Beauchamp-Mustafaga 2024: 4). CDO focuses on affecting an adversary's cognitive abilities and reflects a broader evolution in PLA military theory, which now views warfare as occurring across three key domains: the physical domain (物理域), the information domain (信息域), and the cognitive domain (认知域). Related concepts are "cognitive warfare" (认知战), "cognitive confrontation" (认知对抗), "cognitive deterrence" (认知威慑), and "command of cognition" (制认知权). A group of PLA researchers argues that the cognitive domain is the new focal point of warfare (Chen 2022; Zhao 2022; Pu et al. 2023). However, this perspective seems not yet to be the official stance of the PLA (Beauchamp-Mustafaga 2024: 3).

Within CDO, there are four main aspects: "reading the brain" (读脑), "controlling the brain" (制脑), "resembling the brain" (类脑), and "strengthening the brain" (强脑). “*Reading the brain*” focuses on understanding how others are thinking, “*resembling the brain*” is about using the human brain as inspiration for designing better computers, and “*strengthening the brain*” is about improving one’s own cognition and performance. “*Controlling the brain*” focuses on influencing or even controlling adversary thinking and behaviour. Although some discussions of "controlling the brain" are speculative and futuristic, practical applications include the PLA’s interest in non-lethal, non-kinetic body-targeted weapons, such as directed energy capabilities (Beauchamp-Mustafaga 2024: 4).

The PLA’s discussions of CDO intersect with concepts like "intelligentized public opinion warfare" (智能化舆论战), which emphasizes the use of AI, big data, social media, and social bots (社交机器人) for more effective messaging and targeting. This includes the creation of "synthetic information" (合成信息)—inauthentic content based on some amount of original information—and the distribution of such content using algorithmic agents. Additionally, the PLA is exploring the idea of "precision cognitive attacks" (精准认知攻击) that rely on "personalized user portraits" created using big data to analyse individual preferences. These attacks aim to create or reinforce "information cocoons" (信息茧房), or information bubbles, which serve to further polarize and divide society by undermining mainstream values.

4. Information Manipulation Outlooks in China and Russia: Comparison and Contextualisation

Russia and China have been singled out as the main threat actors that wage FIMI campaigns against the EU, and the West in general, challenging the liberal international order. These campaigns are inextricably linked 1) with the nature and preservation of their political regimes and 2) with the goals the two states pursue both domestically and internationally. Domestically, Russia's political system may be characterized as competitive authoritarianism/autocracy, whereas China's is a one-party communist rule. They are both suspicious of and hostile towards the liberal democratic model which is perceived as threatening their regimes. Thus, their regime stability and state security depend on defending themselves from the spread of liberal democratic values, on how they portray/promote themselves abroad, and, particularly in the case of Russia, on interfering in the information space and domestic affairs of democratic states. Internationally, Russia is a revisionist state that seeks to regain its great power status in global politics. China, on its part, uses its economic clout to exert political power in the international system. However, there are also strategic differences between Russia and China. For Moscow, the EU plays a much more central role, while Beijing's focus is more on nearby regions like Taiwan and the South China Sea.

In recognizing the importance of timely detection and counteraction, the EEAS has developed the concept of FIMI as a structured framework for defence against foreign influence and disinformation. Comparing the Chinese and Russian doctrines, on the one hand, and the EEAS FIMI framework, on the other, shows conceptual differences regarding FIMI and the strategic use of information/disinformation.

4.1. Similarities of Russia and China on Information Manipulation Conceptualisation

Russia and China, two of the world's foremost global powers, share similar approaches to foreign information manipulation and interference (FIMI), driven by their aspirations to

establish dominance in the global information space as evinced in a number of state documents and scholarly literature. The reviewed documents identify the dimensions of FIMI, disinformation and propaganda concepts in Russian and Chinese military doctrines.

The documents reveal Russia's and China's **aspirations and strategic goals**. Both countries display **urgency of being a power in the global information sphere**. Under this framework of information competition and warfare, both Russia and China aspire to dominate and have strong international presence in the global information sphere, in order to both promote their narratives and contest the rival ones. Their goals are to seek global influence through strategic information dominance. Discourse and power, under this framework, are sources of national power in an age of geopolitical competition. Russia, according to its documents, aims to establish itself as a dominant power in the global information space and position itself among global ICT leaders. Its focus is on strengthening technological capabilities for influence. China, through the CCP's operations, is more focused on the strategic level, aiming to correct Western misperceptions and promote China's narrative both domestically and internationally.

The **perception of Western influence as a direct threat** to their regimes by both China and Russia is key to understanding the conceptual framing and the intensity of their FIMI strategies. One of the core similarities between the two is their shared **perception of being the victim** of and under attack by Western countries, particularly the US, which would have used a variety of channels to undermine Russia and China, in order not only to destabilize the existing regimes (framing it as a battle between democracies against autocracies), but also to geopolitically stop Russia and China from rising as powers in the international system and threaten the United States hegemony. Therefore, they frame their actions in the information sphere as a response to an offensive attack by Western countries, and the engagement in certain information tactics as a necessary and proportionate response. Russia believes the collective West is engaged in a concerted hybrid warfare campaign to destabilize it through corrupting its core values and its society. In seeking to preserve these values, it is bent on countering the attempts to impose pseudo-humanistic or other neoliberal ideological views. China also fears Western efforts to infiltrate its ideology and transform the Chinese regime into one that is more desirable for the West by promoting liberal values, human rights and democracy. For China, Western interference as an ideological infiltration aims to weaken

the Chinese Communist Party's control. With respect to this, China conceptualizes FIMI as a defensive response. Differentiating the two, Russia emphasizes narratives about Western-led destabilization, while China focuses more on cognitive threats.

Both **Russia and China frame their efforts as defensive** to counter Western propaganda and react to perceived Western threats. Russia often frames its actions as defensive, using defensive language to mask or justify offensive operations. It perceives itself as a victim of Western aggression and hybrid warfare. China, too, primarily sees its information activities as a defence against Western ideological infiltration, conceptualizing FIMI efforts as necessary for regime security and cognitive security. A deeper analysis of their narratives, however, reveals that there is a high degree of **offensive posturing**, all the more that information is consistently conceived of and used as a weapon.

Another commonality is their **perception of information as a political and military weapon**. The **"weaponization"** of disinformation and propaganda by China and Russia is an important feature of their military doctrines. Russia and China understand the information space as one of the main fields of political contestation and military conflict. Both countries share a perception of modern wars increasingly being focused on information, an asset that both China and Russia perceive has been weaponized by Western governments and therefore they should respond by strengthening their own information offensive and defensive capabilities. They both conceptualize and use information as a weapon to influence adversaries' perceptions and behaviours. **Information, generally, is seen as critical on the internal and external fronts (and diaspora).** Both countries frame the information competition as critical both in foreign policy terms and for stability and fighting internal enemies in their own territory. They also explicitly mention their diaspora abroad as a field of action both in defensive and offensive terms.

Information warfare is also viewed as psychological warfare. Both countries have analysed information from the psychological and cognitive dimensions, as a tool that can generate positive and negative emotions in individuals and groups. This individual-psychological dimension is integrated into the vision of information warfare of both countries. Russia, in particular, views information as a tool for military, political, and psychological influence, with a focus on eroding adversaries' cohesion and destabilizing their societies. China, on its part, operates under the concept of the "Three Warfares" (psychological, media,

and legal warfare), using information to manipulate adversaries' perceptions and will to fight, often with a focus on public opinion warfare. The “Three Warfares” doctrine uses a more structured approach compared to the Russian doctrine, which emphasizes military and psychological operations.

This links to the perception of Russia and China on **weaponization of media outlets, soft power, human rights and democracy promotion** as both governments share the view that international Western media is a tool through which Western governments aim to erode the legitimacy and stability of the Russian and Chinese regime. They also include in the perceived hybrid offensive actions such as soft power, promotion of human rights and democracy promotion initiatives.

On the **media and public opinion** front, the two countries engage in controlling public opinion and leveraging media to further their narratives by presenting “truthful” information, forming perceptions and promoting their own perspectives. China uses public opinion warfare as a core tactic, leveraging media to weaken adversaries' will while promoting China's global discourse power. Russia seeks to influence public opinion domestically and internationally, using state-controlled media to propagate the official narrative. Nevertheless, they exhibit some differences as China focuses more on controlling and shaping international discourse power, while Russia emphasizes safeguarding its tradition and conservative values.

Russia and China attach considerable **importance to create a positive image abroad**, aiming to control their international image through **strategic narratives**, which they disseminate in a structured and focused manner across the target countries. Moscow engages in shaping international perceptions of Russia through propaganda, aiming to counteract negative perceptions and perceived anti-Russian campaigns and to promote an image of strength. Beijing works to proactively promote China's narrative on the global stage, seeking to reshape global discourse, to “tell China's story well” internationally and to establish dominance by promoting its own narrative. Both governments have framed their information strategies not only in defensive and reactive terms but also stressing the importance of promoting a positive image abroad through their international media ecosystem. It is relevant to underline that both governments, even in the current age of social media, still consider traditional media and diplomatic channels as strongly important tools.

The **technological use of information** is considered an important facet of the FIMI efforts of China and Russia as they attempt to apply and leverage advanced technologies for disinformation and influence. China frames its FIMI conception in a more high-tech language compared to Russia. It focuses more on technological sophistication and uses advanced technologies like AI, big data, and social media. The effective messaging relies on creating and reinforcing information cocoons. Russia, on the other hand, strengthens its use of information and telecommunications technologies as weapons, with a focus on broader cyber capabilities to protect national interests.

A significant driver of both Russia's and China's FIMI tactics is the goal of ensuring **regime security and national stability**. To achieve this goal, information control and manipulation are employed. For Russia, information security is framed as critical to safeguarding national security and defending against external threats, and more broadly – internal stability by focusing on protecting internal values and ensuring a secure information space. China, in contrast, emphasizes cognitive domain operations to protect its regime security, with a focus on information security that prevents ideological subversion. Thus, regime security and stability is linked to **values and ideology**. Russia and China not only consider regime security and stability - and in broader terms, national security - as one of the main goals of engaging in information competition, but they also consider the maintenance of certain values as critical, Russia conceptualises it as a defence of traditional and national values, and China frames it in terms of ideological contestation.

Overall, despite the many similarities and the fact that security concerns seemingly dominate in both countries' military doctrines, there are some **differences** in content, style and language to be noted. In sum, the military doctrines of Russia and China with their FIMI components display different discursive content and language. China uses more militarized and high-tech language, whereas Russia uses predominantly geopolitical and power politics discourse. What is more, China's FIMI is conceptualized mostly in scientific-psychological/cognitive terms compared to Russia's more values-oriented approach. Importantly, whereas China frames its conception of FIMI predominantly in terms of war and warfare, Russia conceptualizes it predominantly in terms of protecting values and traditions.

Russia as a revisionist state is led by the desire to be recognized as a great power. Therefore, its FIMI concept is framed largely in **geopolitical terms**. Russia's doctrine seems

conceptualized primarily in terms of the structure of the international system (multipolarity) and the need to establish a new world order, with strategic and geopolitical overtones. In contrast, China's concept seems more foreign policy-oriented with an explicit emphasis on cognitive operations. China is more oriented towards **foreign and military policy** with the active participation of party and state structures.

4.2. Differences of the Russian and Chinese conceptualisation in comparison to the EEAS FIMI framework

The EEAS model of FIMI represents 1) an analytical framework for FIMI threat analysis, and 2) a response framework to FIMI threats. The EEAS framework is thus entirely defensive with an objective to detect, interrupt/disrupt/break and counteract subversive influence and information manipulation. Compared to the EEAS FIMI framework, the Russian and Chinese documents consider information warfare as part of their military doctrines and they reveal an offensive posture.

Based on a comparison of the conducted archival work on Russia and China and the existing FIMI-related documents of the European External Action Service (EEAS), several conclusions can be drawn about the differences in their approaches to FIMI.

First, when it comes to **core priorities and values**, while all three actors - Russia, China, and the European Union – have framed in defensive terms their participation in information competition or counter-FIMI actions, what they claim to be defending is notably different. Russia and China state that they defend national sovereignty and regime stability, while the EEAS frames its actions as defending democracy and the liberal political system. While all parties present their actions as defending values, Russia and China focus on traditional or ideological values, whereas the EEAS emphasizes the defence of democratic values. It is important to note that both Russia and China frame their values as national and idiosyncratic, while the EEAS frames democratic values within the universalist liberal tradition.

The **role of the media** is another area where the framing differs significantly. Russia and China perceive the media as both a weapon and a counter-weapon in the ongoing information competition and warfare, and therefore perceive their own media as an asset in the present

information war. By contrast, the EEAS views the media in the context of media pluralism and transparency, considering media outlets as independent from government power, rather than as an extension of it.

The **geographical dimension** also varies. Russia and China conceptualize the international information competition in global terms, emphasizing the importance of becoming global information powers. However, the EEAS focus is more regional, concentrating on FIMI actions within the EU and its immediate neighbourhood, rather than globally.

The focus of analysis in terms of **narrative or behaviour** in these documents also varies between the actors. Most Russian and Chinese documents dedicate more attention to the content and narrative aspects of information competition. In contrast, the EEAS, under the FIMI framework, focuses more on the behaviour of the actors involved, such as their tactics, techniques, and procedures (TTPs), which highlights a more process-oriented approach.

Another divergence is in the **psychological and cognitive domain**. Russia and China consider the psychological and cognitive aspects as critical areas of contestation. In comparison, the EEAS does not place significant emphasis on these dimensions.

In addition, Russia and China highlight the need to respond to perceived threats with **actions in the adversaries' territory**. Russia and China explicitly state their intention to conduct information operations in the territory of their perceived adversaries, targeting the populations of Western countries. The EEAS, however, does not include in its responses counterattacks within rival territories. Instead, its focus is on deactivating FIMI operations that affect the EU or its member states.

Finally, Russia and China mention their **diaspora** populations abroad as critical targets that must be defended from Western information operations. As such, they see it as legitimate to conduct information operations in third countries, including Western countries where significant diasporas reside. In contrast, European diasporas abroad do not play a role in the EEAS FIMI strategy.

In sum, these points underscore the contrasting priorities, tactics, and geographical scopes that define Russia and China's more globally assertive and ideologically framed information warfare strategies, compared to the EEAS's more regionally focused, behaviour-oriented,

and defensive approach aimed at protecting democratic values and institutions within the EU. While all three actors engage in information competition, Russia and China focus on defending national sovereignty, traditional values, and global influence, using media as a tool of state power and projecting their actions abroad. The EEAS, on the other hand, emphasizes defending democratic values, focusing on media independence and regional threats, with a priority on actor behaviour rather than content or narratives.

In the pursuit of their national goals and aspirations, China and Russia employ various strategies to spread disinformation and propaganda in their quest to dominate the international information space. The FIMI dimension of their doctrines, as elaborated in the reviewed documents, indicates their intentions in global politics and highlights the strategic importance of FIMI as a foreign policy instrument. Both countries operate in various contexts, providing grounds for further research at different levels of analysis (e.g., international relations, foreign policy, and security). These frameworks also offer avenues for extensive future research on the interplay of FIMI and power dynamics in the international system, potentially explaining the objectives of Russia and China as threat actors.

5. References

Academy of Military Science Military Strategy Research Department [军事科学院军事 战略研究部], eds., *The Science of Military Strategy* [战略学]. Military Science Press, 2013

Aischmann, F. (March 31, 2023). Russland neue Außenpolitik-Doktrin - der Westen als Feind, Russland als Opfer. tagesschau.de. https://www.tagesschau.de/ausland/russland-ukraine-krieg-sicherheitspolitik-putin-usa-101.html

Beauchamp-Mustafaga, Nathan. 2023. “Chinese Next-Generation Psychological Warfare: The Military Applications of Emerging Technologies and Implications for the United States.” RAND Corporation. https://www.rand.org/pubs/research_reports/RRA853-1.html.

Beauchamp-Mustafaga, Nathan. 2024. “Exploring the Implications of Generative AI for Chinese Military Cyber-Enabled Influence Operations: Chinese Military Strategies, Capabilities, and Intent.” RAND Corporation. https://www.rand.org/pubs/testimonies/CTA3191-1.html.

Cao Hong (蔡虹), “A Study on the Strategy of "Borrowing Ships to Go to Sea" in External Communication “ (对外传播之 ‘借船出海’ 策略研究), The Press (新闻战线), 1.1.2020. http://paper.people.com.cn/xwzx/html/2020-01/01/content_2002728.htm.

CCPCC, “CCP Central Committee Issues Regulations on the Work of the Unified Front of the Communist Party of China.” 05.01.2021. https://www.spp.gov.cn/dj/c100027/202101/t20210105_505639.shtml.

Chen Dongheng (陈东恒), “Command of Cognition: An Important Support for Winning the War” (制认知权: 战争制胜重要支撑), PLA Daily, April 19, 2022

Clay, Marcus, and Roderick Lee. 24.01.2022. “Unmasking the Devil in the Details- A Comparative Analysis of the Science of Military Strategy 2017 and 2020 > Air

University (AU) >." *China Aerospace Studies Institute*. https://www.airuniversity.af.edu/CASI/Display/Article/2901441/unmasking-the-devil-in-the-details-a-comparative-analysis-of-the-science-of-mil/.

Cull, N. J. (2009). The cold war and the United States information agency: American propaganda and public diplomacy. Cambridge University Press.

Council of the European Union. *EU sanctions against Russia over Ukraine (since 2014).* https://www.consilium.europa.eu/en/infographics/eu-sanctions-against-russia-over-ukraine/

Doktrina informatsionnoy bezopasnosti Rossiyskoy Federatsii ot 5 dekabrya 2016 g. №646. https://mid.ru/ru/foreign_policy/official_documents/1539546/?lang=ru

European External Action Service. (2024). *2nd EEAS Report on Foreign Information Manipulation and Interference Threats: A Framework for Networked Defence.* https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report%20on%20FIMI%20Threats-January-2024_0.pdf

European External Action Service. (2025). *3rd EEAS Report on Foreign Information Manipulation and Interference Threats: Exposing the architecture of FIMI operations.* https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf

Fravel, Tylor M. (2019). *Active Defence: China's Military Strategy since 1949.* Princeton, NJ: Princeton University Press.

Filonenko, L. V., Agapova, G. V., & Prilepina, N. V. (2024). Tekhnologii Organizatsii i Provedeniya Raboty po Informatsionnoy i Psikhologicheskoy Bezopastnosti Lichnosti Voyennosluzaschich. Vozdushno-kosmicheskiye sily. Teoriya i praktika, (29), 126-137.

Gaufman, Elizaveta. 2017. "(Re)Drawing Boundaries: Russia and the Baltic States." In Borders in the Baltic Sea Region: Suturing the Ruptures, edited by Andrey Makarychev and Alexandra Yatsyk, 249–68. London: Palgrave Macmillan UK. https://doi.org/10.1057/978-1-352-00014-6_11.

Gerasimov, V. (2013). *The Value of Science Is in the Foresight New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations.* Originally published in Military-Industrial Kurier, 27 February 2013. Translated from Russian 21

June 2014 by Robert Coalson, editor, Central News, Radio Free Europe/Radio Liberty. https://www.armyupress.army.mil/portals/7/military-review/archives/english/militaryreview_20160228_art008.pdf

Gereykhanova, A. (February, 9, 2024). Putin rasskazal Karlsonu ob istorii poyavleniya Rossii i Ukrainy. Rossiyskaya gazeta. https://rg.ru/2024/02/09/putin-rasskazal-karlsonu-ob-istorii-poiavleniia-rossii-i-ukrainy.html

Harold, Scott W., Nathan Beauchamp-Mustafaga, and Jeffrey W. Hornung. 2021. “Chinese Disinformation Efforts on Social Media.” RAND Corporation. https://www.rand.org/pubs/research_reports/RR4373z3.html.

Høiback, Harald. 2011. “What Is Doctrine?” Journal of Strategic Studies 34 (6): 879–900. https://doi.org/10.1080/01402390.2011.561104.

Høiback, Harald. 2016. “The Anatomy of Doctrine and Ways to Keep It Fit.” Journal of Strategic Studies 39 (2): 185–97. https://doi.org/10.1080/01402390.2015.1115037.

Il'ichev, A. V. 2023. Diskurs gibridnoy voyny kak mekhanizm formirovaniya negativnogo obraza Rossii. Konfliktologiya/nota bene, (3), 36-53.

Kania, Elsa. 2016. “The PLA’s Latest Strategic Thinking on the Three Warfares.” *China Brief.* 16 (3). https://jamestown.org/program/the-plas-latest-strategic-thinking-on-the-three-warfares/.

Kiselev V. 2015. " Gibridnaâ vojna kak novyj tip vojny budušego [Hybrid War as a new type of a future war]." Armejskiy Sbornik 12.

Kontseptsiya gosudarstvennoy politiki Rossiyskoy Federatsii v sfere sodeystviya mezhdunarodnomu razvitiyu utv. Ukazom Prezidenta RF ot 20 aprelya 2014 g. N 259. https://mid.ru/ru/foreign_policy/official_documents/1584961/?lang=ru

Kontseptsiya vneshney politiki Rossiyskoy Federatsii ot 12 iyulya 2008 g. N Pr-1440. https://normativ.kontur.ru/document?moduleId=1&documentId=131926

Kontseptsiya vneshney politiki Rossiyskoy Federatsii ot 11 iyulya 2000 g. Via link from Nezavisimaya Gazeta: https://www.ng.ru/world/2000-07-11/1_concept.html

Kontseptsiya vneshney politiki Rossiyskoy Federatsii ot 12 fevralya 2013 g. Via link from Garant.ru: https://www.garant.ru/products/ipo/prime/doc/70218094/

Kontseptsiya vneshney politiki Rossiyskoy Federatsii utverzhdena Prezidentom Rossiyskoy Federatsii V.V. Putinym 31 marta 2023 g. https://mid.ru/ru/foreign_policy/official_documents/1860586/?lang=ru

Lepsky, Vladimir. Informatsionno-psikhologicheskaya bezopasnost' sub"yektov diplomaticheskoy deyatel'nosti / Diplomaticheskiy yezhegodnik - 2002. Sbornik statey. Koll. avtorov. - M.: Nauchnaya kniga. 2003. S.233-248.

Livingston, S. (1997). CLARIFYING THE CNN EFFECT: An Examination of Media Effects According to Type of Military Intervention. The Joan Shorenstein Center on the Press, Politics and Public Policy, Harvard University John F. Kennedy School of Government. Research Paper R-18.

Makashova, V. V. (2023). DEZINFORMATSIYA Kak Element Tekhnologiy Upravleniya Smyslami. MediaVektor, (9), 84-88.

Manoylo A.V. Gosudarstvennaya informatsionnaya politika v osobykh usloviyakh: Monografiya. M.: MIFI, 2003

Manoylo, A. V. (2018). Informatsionnyye voyny i psikhologicheskiye operatsii. Rukovodstvo k deystviyu. M.: Goryachaya liniya-Telekom

Manoylo, A. V. (2021). Evolyutsiya informatsionnykh operatsiy. Rossiyskiy sotsial'no-gumanitarnyy zhurnal, (4), 80-103.

Markov, Yevgeniy, and Nevolina, Anna. 2018. " Rossiâ kak glavnyj ob"ekt sovremennyh informacionnyh vojn [Russia as the main target of modern information wars]." Historia provinciae – žurnal regional'noy istorii 2 (3).

OVD-Info. “Persecution of the Anti-War Movement Report. May-September 2024.” n.d. Accessed June 1, 2025. https://ovd.info/en/persecution-anti-war-movement-report-may-september-2024.

Pomerantsev, P. and Weiss, M. (2014). *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money.* Institute of Modern Russia, Inc. Page 6. https://bit.ly/3VQ3nuR

PRC Central People's Government, "CCP Central Committee, State Council, and Central Military Commission Print and Distribute 'Opinion on the Integrated Development of Economic and Defense Construction.'" 21.07.2016. https://www.gov.cn/xinwen/2016-07/21/content_5093488.htm.

Pu Duanhua (濮端华), Li Xiwen (李习文), and Xiao Fei (肖飞), "Getting It Right on How Cognitive Penetration Influences Multi-Domain Operations" (把准认知域渗透影响多域作战的规律), PLA Daily, January 19, 2023.

Putin, V. (2007). Prepared Remarks at 43rd Munich Conference on Security Policy. *Washington Post (transcript).* https://bit.ly/4g67rkp

Radnitz, S. (2022). Dilemmas of distrust: Conspiracy beliefs, elite rhetoric, and motivated reasoning. Political Research Quarterly, 75(4), 1143-1157.

"Regulations on the Political Work in the PLA" (军队政治工作条例), revised in 2021. Earlier versions 2003 and 2013.

Samokhvalova, Vera. 2011. "Specifika sovremennoj informacionnoj vojny: sredstva i celi poraženiâ [The specifics of modern information warfare: the means and targets of destruction]." Filosofiâ i obŝestvo (3): 54–73.

Sherstoboyeva, E. (2024). Russian Bans on 'Fake News' about the war in Ukraine: Conditional truth and unconditional loyalty. *International Communication Gazette*, *86*(1), 36-54.

Smirnov, A. (2013). Informatsionno-psikhologicheskaya voyna. Svobodnaya mysl', (6), 81-96.

Smolyan, G. L., Voyskunskiy, A. Ye., Zarakovskiy, G. M., & Rozin, V. M. (1996). Informatsionno-psikhologicheskaya bezopasnost' (opredeleniye i analiz predmetnoy oblasti) (No. 96-06-80040). Rossiyskiy fond fundamental'nykh issledovaniy.

State Council Information Office, China's Military Strategy, May 27, 2015.

Strategiya razvitiya informatsionnogo obshchestva v Rossiyskoy Federatsii ot 7 fevralya 2008 g. N Pr-212. https://mid.ru/ru/foreign_policy/official_documents/1691980/

Strategiya natsionalnoy bezopasnosti Rossiyskoy Federatsii ot 02 iyulya 2021 g. https://mid.ru/ru/foreign_policy/official_documents/1784948/

Tang Aijun (唐爱军), "Ideological Security in the Framework of the Overall National Security Outlook" (总体国家安全观视域中的意识形态安全). Translated by CSIS Inerpret: China. *Socialism Studies*. 12.12.2019. https://interpret.csis.org/translations/ideological-security-in-the-framework-of-the-overall-national-security-outlook/.

Tosi, Scott J. (2023). "Xi Jinping's PLA Reforms and Redefining 'Active Defense'". *Military Review*, September/October 2023. https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/September-October-23/Active-Defense/Active-Defense-UA1.pdf

Ukaz Prezidenta RF ot 30 noyabrya 2016 g. N 640 "Ob utverzhdenii Kontseptsii vneshney politiki Rossiyskoy Federatsii." Via link from Garant.ru: https://base.garant.ru/71552062/#block_1000

U.S. Department of State. (2014). *Ukraine and Russia Sanctions.* https://2009-2017.state.gov/e/eb/tfs/spi/ukrainerussia/

Vladimirov, Aleksandr 2013. Osnovy obŝej teorii vojny. Čast' I: Osnovy teorii vojny [Foundations of common war theory. Part I, Foundations of War Theory]." Kadet.ru.

Voennaya doktrina Rossiyskoy Federatsii v redaktsii ot 25 dekabrya 2014 g. https://mid.ru/ru/foreign_policy/official_documents/1584621/

Wu Jieming (吴杰明) and Liu Zhifu (刘志富), *An Introduction to Public Opinion War- fare, Psychological Warfare, [and] Legal Warfare* (舆论战心理战法律战概论), Na- tional Defense University Press, 2014.

Xi Jinping (习近平), "Fully, Accurately and Comprehensively Implement the Important Thoughts on Doing the Party's United Front Work Well in the New Era" (完整、准确、全面贯彻落实关于做好新时代党的统一战线工作的重要思想), *Qiushi* (求是), No. 2, 2024. http://www.qstheory.cn/dukan/qs/2024-01/15/c_1130059591.htm.

Xinhua, "In His Address to the 30th Group Study Session of the CCPCC Politburo, Xi Jinping Stressed the Need to Strengthen and Improve International Communication to Display the True, Three-Dimensional and Comprehensive China" (习近平在中共中央政治局第三十次集体学习时强调: 加强和改进国际传播工作, 展示真实立体全面的中国), 01.06.2021. http://www.xinhuanet.com/politics/leaders/2021-06/01/c_1127517461.htm.

Xinhua, "Xi Jinping: Telling China's Story Well, Making China's Voice Heard" (习近平：讲好中国故事 传播好中国声音), 21.08.2013. http://www.xinhuanet.com/zgjx/2013-08/21/c_132648439.htm.

Xiao Tianliang (肖天亮), ed., *Science of. Military Strategy* (战略学) (Beijing: National Defense University Press (国防大学出版社), 2020).

Yamaguchi, Shinji, Masaaki Yatsuzuka, and Rira Momma. 2023. *China's Quest for Control of the Cognitive Domain and Gray Zone Situations*. NIDS China Security Report. National Institute for Defense Studies, Japan. https://www.nids.mod.go.jp/publication/chinareport/pdf/china_report_EN_web_2023_A01.pdf.

Yablokov, I. (2018). Fortress Russia: Conspiracy theories in the post-Soviet world. John Wiley & Sons.

Zarudnitskiy, V. B. (2023). Sovremennyye voyennyye konflikty v kontekste formirovaniya novoy geopoliticheskoy kartiny mira. Voyennaya mysl', (11), 6-15.

Zhang Yuliang (张玉良), ed., The Science of Campaigns (战役学), Beijing, China: National Defense University Press, 2006.

Zhao Quanhong (赵全红), “Cognitive Domain Operations: The Key to Winning Modern Warfare” (认知域作战：现代战争的制胜关键), PLA Daily, July 14, 2022

Zhu Xueling (朱雪玲) and Zeng Huafeng (曾华锋), “Mind Control Operations: New Model of Future Wars” (“制脑作战:未来战争竞争新模式), PLA Daily, October 17, 2017, http://www.81.cn/jfjbmap/content/2017-10/17/content_189879.htm.

Zhang Yuliang [张玉良], ed., The Science of Campaigns [战役学], Beijing, China: National Defense University Press [国防大学出版社], 200

DE-CONSPIRATOR

DETECTING AND COUNTERING INFORMATION SUPPRESSION FROM A TRANSNATIONAL PERSPECTIVE

GA 101132671

info@deconspirator-project.eu

www.deconspirator-project.eu

Partners

AdCogito

CSD Center for the Study of Democracy

CIDOB Barcelona Centre for International Affairs

edam Centre for Economics and Foreign Policy Studies

University of Georgia

Universität Heidelberg Zukunft seit 1386

Istituto Affari Internazionali

Özyeğin University

rijksuniversiteit groningen

Rīga Stradiņš University

University of Amsterdam

VUB Vrije Universiteit Brussel

WHITE

Funded by the European Union