Ref. Ares(2025)5089187 - 26/06/2025

DE-CONSPIRATOR

DETECTING AND COUNTERING INFORMATION SUPPRESSION FROM A TRANSNATIONAL PERSPECTIVE

D2.2

A Glossary of FIMI-Related Terms

Under EC Review

IAI

03/06/2024

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, Istanbul, 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.

Under EC Review

LEGAL NOTICE

The information and views set out in this report are those of the authors and do not necessarily reflect the official opinion of the European Union. Neither the European Union institutions and bodies nor any person acting on their behalf may be held responsible for the use which may be made of the information contained therein.

© DE-CONSPIRATOR Consortium, 2024-2026

Reproduction is authorised provided the source is acknowledged.

Grant Agreement: 101132671 | Coordination and Support Action | 2024 – 2026 | Duration: 36 months

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

Document Information

DX.Y: Title of deliverable:	A Glossary of FIMI-Related Terms
Issued by:	IAI
Issue date:	03/06/2024
Due date:	30/04/2024
Work Package Leader:	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)	

Under EC Review

Version Control Sheet

Version	Date	Main modifications	Organisation
0.1	27.04.2024	First version of the document	IAI
1.0	03.06.2024	Minor changes have been made regarding the content and the formatting	IAI, EDAM, OzU
1.1	15.04.2025	Revisions have been made based on the reviewers feedbacks and shared with partners to contribute.	IAI, EDAM
2.0	03.06.2024	Final Version	IAI, EDAM

Main Authors

Name	Organisation
Aurelio Insisa	IAI
Nona Mikhelidze	IAI

Quality Reviewers

Name	Organisation
Zeynep Alemdar	EDAM
Sinan Ülgen	EDAM
Alina İltutmuş	EDAM
Akın Ünver	OzU
Azade Eryiğit	OzU

Under EC Review

Table of Contents

Under EC Review

Under EC Review

Under EC Review

EXECUTIVE SUMMARY

This glossary presents a comprehensive list of tactics, techniques, and procedures (TTP) related to Foreign Information Manipulation and Influence (FIMI). The list includes TTPs that have been conceptualised within the academic, policy, and military milieus of Europe, the Anglosphere, and Japan to describe general modes of action, or those specific to China and Russia. It also includes TTPs conceptualised within Chinese and Russian academic, policy, and military milieus to address these countries' actions, as well as those of the collective "West".

While available to the public, this glossary is conceived as an internal tool for the researchers of the DE-CONSPIRATOR consortium. All the sources consulted to draft the glossary are available in the appendix. Readers interested in using a TTP definition for academic research are invited to consult the relevant sources listed in the appendix.

Terms written entirely in capital letters identify TTPs that have their own distinct entry in the glossary. Example: **HYBRID WARFARE**. Bold characters without capital letters are used for different monikers of the same TTP. Example: **hybrid threats**. Quotation marks are used for TTPs that are primarily known via idiomatic expressions and their eventual translations in English.

Under EC Review

THE GLOSSARY

ACTIVE MEASURES (активные мероприятия, *aktivnye meropriyatiya*). The term refers to techniques and tactics of POLITICAL WARFARE historically used by the intelligence services of the Soviet Union to undermine the political interests of adversary nations, weaken their positions, and disrupt their plans. Comparable to U.S. covert actions, active measures involve the manipulation of media, societies, and political processes through PROPAGANDA, paramilitary and clandestine actions, and the strategic use of intelligence.

ALGORITHMIC BIAS The systematic and repeatable distortion in algorithmic systems that produces outcomes favouring or disadvantaging certain groups, individuals, or perspectives. Algorithmic bias can arise from biased training data, flawed design choices, or the unintended consequences of optimization goals, leading to discriminatory effects in areas such as content visibility, decision-making, and information dissemination.

"BORROWING A BOAT TO GO OUT TO SEA" (接船出海, *jiechuan chuhai*). A Chinese tactic aiming at using popular and/or respected foreign media to deliver Chinese narratives to foreign audiences.

BOTNETS Networks of automated accounts, or bots, programmed to spread messages on social media without human intervention, serving as amplifiers for DISINFORMATION CAMPAIGNS. Botnets exploit online anonymity, making it difficult to discern human versus automated speech. Botnets may be effective because of the volume and speed of the dissemination of their outputs, but also for the convincing quality of audio-visual content of the messages they disseminate.

CENSORSHIP The act of controlling the flow of information and suppressing content for political and ethical reasons. While commonly associated with totalitarian regimes and top-down enforcement by state authorities, forms of censorship are present in virtually any type of political regime, including liberal democracies. Within contemporary authoritarian regimes' censorship**,** is usually selective and strategic, rather than exercising a blanket ban on content deemed "problematic". Such an approach allows monitoring of public sentiment more effectively. **Digital censorship** entails the removal or obscuring of internet content accessible to the public, as well as restrictions on one's ability to transmit information digitally to a wider audience.

COGNITIVE WARFARE A term commonly used in Western and global media to describe China's INFORMATION WARFARE and PSYCHOLOGICAL WARFARE, especially targeted against Taiwan, since the late 2010s. People's Liberation Army literature uses instead the term **cognitive domain operations** (认知域作战, *renzhiyu zuozhan*) to describe an operational concept focused on the application of artificial intelligence and big data to psychological warfare (here to be understood as a component of the THREE WARFARES) with the aim to manipulate opponents' cognitive and decision-making processes.

COMPETITIVE STRUGGLE (конкурентная борьба, *konkurentnaya borba*). A foundational concept in Russian foreign policy that frames international relations in terms of a zero-sum contest for power. Russia sees itself as an emerging power challenging Western dominance, with the West, led by the USA, perceived as obstructive to the country's legitimate interests. This competition involves undermining rivals to strengthen one's own position, with the information domain as a critical battleground. Russia perceives Western media as tools used to attack and undermine its interests, prompting the development of defensive and counterattack measures.

COMPOUND WARFARE A conceptualisation of warfare that emerged in the U.S. in the early 2000s, based on the simultaneous use of "regular" and "irregular" forces against an enemy, with the aim to generate an

Under EC Review

impact that is greater than the sum of its parts. The deployment of irregular forces provides an opening for the use of INFORMATION OPERATIONS, and more broadly for INFLUENCE ACTIVITIES, outside of the battlefield. Compound warfare can be considered the predecessor of HYBRID WARFARE, a concept that would become popular in 2010s.

CONSPIRACY THEORIES Conspiracy theories are lay beliefs that attribute the ultimate cause of an event or the concealment of an event from public knowledge to a secret, unlawful, and malevolent plot by multiple actors working together. Belief in conspiracy theories among certain audiences can be exploited by adversaries, who can tailor narratives to fit such beliefs and facilitate their dissemination.

CONTENT MODERATION The processes and practices by which digital platforms monitor, evaluate, and manage user-generated content in accordance with legal requirements, community standards, or corporate policies. It involves decisions about what content is allowed, restricted, removed, or deprioritized, and can be carried out manually by human moderators or automatically through algorithmic systems. While often intended to prevent harm, MISINFORMATION, or illegal activity, content moderation also raises critical questions about free expression, political bias, and accountability. In both democratic and authoritarian contexts, moderation practices can inadvertently or deliberately lead to the suppression of certain voices or viewpoints, making it a central concern in debates over digital governance and platform power.

CYBERATTACKS Deliberate actions that target the availability, integrity, and/or protection of data or information systems. Sensitive information that is obtained through cyberattacks may enable INFORMATION OPERATIONS against an adversary. A confrontation by state or state-adjacent actors conducting these types of attacks against an adversary to achieve politico-military objectives is more commonly defined as **cyberwarfare**.

DEBUNKING A process of exposing false claims, myths, or misconceptions by providing evidence or logical reasoning to refute them. It involves critically examining and discrediting MISINFORMATION or unsupported beliefs.

DEEPFAKES A deepfake is a synthetic video or audio media output, created using artificial intelligence techniques. These techniques are used to manipulate and superimpose existing images or recordings onto source material, often resulting in highly realistic but fabricated content. Deepfakes can be used to create convincing depictions of people saying or doing things they never actually did, raising concerns about their potential use for spreading MISINFORMATION and/or DISINFORMATION and thus manipulating public opinion.

DIGITAL DISRUPTION Digital disruption refers to INTERFERENCE in digital infrastructure or services aimed at creating chaos, confusion, or rendering systems inoperative, thereby undermining social, economic, or political stability. This disruption can occur through various methods, including CYBERATTACKS like Distributed Denial of Service (DDoS) attacks, ransomware, or malware; system infiltration involving unauthorized access and manipulation of data; exploitation of software vulnerabilities; and flooding digital platforms with excessive information (often false and misleading) to overwhelm information processing capacities.

DIGITAL SUBVERSION Digital subversion is the use of digital technology or platforms to undermine established systems, norms, or authority structures. It encompasses various strategies and methods, including hacking, online activism, and DISINFORMATION campaigns.

DISCOURSE POWER (话语权, *huayu quan*). A conceptual platform used in China to conceptualise threats, disadvantages, and objectives for the Chinese Party-State in the INFORMATION SPACE. Chinese interpretation

Under EC Review

of this concept have ranged from "right to speak" (the right to be heard on the international stage notwithstanding the hegemony of international media); as "power discourse" (the growing ability to shape the global information space in relation to the comprehensive growth of a country's national power); as "power of the media" (actual control over the media); as SOFT POWER; and as "diplomatic skill" (namely the ability to use all the tools of diplomacy, including PUBLIC DIPLOMACY, to make China's voice heard globally). Under the Xi administration "discourse power" has evolved into a strategy to support China's rise and guarantee regime security.

DISINFORMATION False or misleading information, either of domestic or foreign origin, that is intentionally crafted and strategically disseminated to achieve a political goal by manipulating an audience's perceptions. Disinformation campaigns often target political actors and/or causes, seeking to undermine their credibility. Tactics used in disinformation campaigns include BOTNETS, TROLL FARMS, and SOCIAL NETWORK MANIPULATION. Disinformation spreads rapidly within closely connected groups, contributing to societal polarization and MISINFORMATION. It has been linked to significant political events and violence worldwide. Coordinated efforts to disseminate disinformation are generally known as **disinformation campaigns**.

FAKE NEWS fully fabricated, partially fabricated, decontextualized stories and other types of content deliberately disseminated by domestic or foreign hostile actors. Fake news often specifically target segments of society that are already prone to discontent (and who may believe in CONSPIRACY THEORIES) or aims to create such discontent and negative perceptions. Fake news can be considered a form of DISINFORMATION or PROPAGANDA.

"FLOODING THE ZONE" The expression "flooding the zone", also known as "info-noise" or *infoshum* (инфошум) in the Russian language, refers to a Russian technique of INFORMATION OPERATIONS, aiming at inundating the INFORMATION SPACE with low-quality content containing diverging information. This tactic aims to obscure genuine news articles, making it difficult for news consumers to access reliable information.

FOURTH-GENERATION WARFARE A conceptualisation of warfare emerging from insurgency, rooted in the assumption that superior political will, when properly employed, can defeat a greater economic and military power. In light of this power asymmetry, the actor that wages this type of warfare makes use of operations within the information domain in order to carry on its fight by directly attacking the cognitive processes of the decision-makers of the opposite actor.

GREY ZONE OPERATIONS Operations in the "grey zone" encompass a wide range of efforts that aim at advancing a political actor's interest against an adversary using means that are at the same time outside of the realm of routine statecraft and below the threshold of direct military confrontation. The concept emerged in the late 2010s in Japanese and US policy and academic milieus to describe Chinese operations in the South and East China Seas and around Taiwan. Grey zone operations are conceptually contiguous but ultimately distinct from HYBRID WARFARE. The latter, however, does not recognise the grey zone's central concept of maintaining operations below the threshold of direct military confrontation.

"HARMONIZATION" (和谐, *hexie*). Term used to describe the CENSORSHIP practices aimed at removing content considered objectionable or destabilising to "societal harmony" as defined by the Chinese government under Hu Jintao's two terms as "paramount leader". Harmonization removes not only politically sensitive content but any type of content that is considered sensitive and potentially divisive from a Chinese socio-cultural perspective. Harmonization relies on the compliance of internet companies as well as on the work of human censors and algorithms.

Under EC Review

HYBRID WARFARE A concept emerging in the 2000s in the U.S. Hybrid warfare was originally defined as the use of different modes of warfare blending regular approaches and irregular approaches that even include terrorist and criminal activity in order to achieve an actor's objective within the battlefield. Since Russia's takeover of Crimea in 2014, the concept's focus in the West has shifted from the battlefield to the full spectrum of great power competition, encompassing any combination of conventional and non-conventional methods to achieve an actor's political-military objective. This shift, in turn, has left an unresolved conceptual tension between "hybrid warfare as a mode of warfare" and "hybrid warfare as a type of strategy". In the second case, hybrid warfare can be understood as a new iteration of POLITICAL WARFARE. Hybrid warfare is also conceptually contiguous to GREY ZONE OPERATIONS. However, hybrid warfare does not imply the necessity to keep operations below the threshold of direct military confrontation. Against this backdrop, the more conceptually flexible term **hybrid threats** has been used instead since the late 2010s. Against this backdrop, the concept of **hybrid interference** defines the deployment of hybrid threats as a wedge strategy, typically used by autocratic states against members of liberal democracies coalitions. The term **hybrid influencing** has been instead used to describe the concerted use of hybrid threats aiming at influencing an adversary's choice in a cognitive environment still permeated by the threat of war. Hybrid warfare and contiguous terms are rarely used in the literature on China but have been widely adopted in the literature on Russia after the partial takeover of Ukraine in 2014. Crucially, within Russia the term ***gibridnaya voyna*** (гибридная война) has been used instead to describe perceived Western (namely American) attempts to erode the socio-cultural cohesion of its adversaries (Russia included) while protecting its own.

IDEOLOGICAL SECURITY Ideological security involves safeguarding a country's dominant ideology from both external and internal threats in order to guarantee national security (and implicitly, regime security). Ideological security provides a conceptual framework for continuing domestic mobilisation, domestic CENSORSHIP, and attempts to suppress sensitive narratives outside national borders. The concept has a transnational appeal for many autocratic regimes across the world and generally frames "the West" as the key source of such threats.

INFLUENCE The ability to shape another actor's perceptions, decision-making processes, and actions in one's favour. Concerted and coordinated attempts to influence a target can be defined either as **influence campaigns** or as **influence operations**. The term broadly encompasses any type of activity – legal and illegal, regular and irregular, overt and covert – across multiple physical and virtual domains. Coercive activities are not generally included within influence activities, even though the potential threat of coercion does play a role in the projection of influence.

INFORMATION ENVIRONMENT A concept central in the STRATEGIC COMMUNICATIONS literature. The information environment is a conceptual space where actors and audiences interact, comprising three interrelated dimensions: the cognitive, physical, and informational dimensions. The inclusion of a cognitive dimension separates it from the more widely used concept of INFORMATION SPACE.

INFORMATION OPERATIONS A term that can be broadly used to describe any type of activity pursued by a political actor in order to achieve its objectives in a contested environment via the dissemination and/or the control of the flow of information. Information operations can consequently be considered as part and parcel of various forms of "warfare" that are not centred on direct kinetic confrontation, such as COGNITIVE WARFARE, COMPOUND WARFARE, FOURTH GENERATION WARFARE, HYBRID WARFARE, LAWFARE, POLITICAL WARFARE, PSYCHOLOGICAL WARFARE, and PUBLIC OPINION WARFARE. They may comprise the execution of CENSORSHIP and/or CYBER ATTACKS; the projection of SHARP POWER; the dissemination of FAKE NEWS, DISINFORMATION, and/or PROPAGANDA, as well as the use of tools such as BOTNETS and TROLLS, and of tactics such as "BORROWING A BOAT TO GO OUT TO SEA" and "FLOODING THE ZONE"; they can be disseminated through traditional mass media and social media**. Informational countermeasures** to information operations may include STRATEGIC COMMUNICATIONS, proactive PUBLIC DIPLOMACY, as well as

Under EC Review

various efforts to raise awareness among the public through warnings, tagging, or identification of suspect source, and through the establishment of new institutions and platforms specifically designed to meet this challenge.

INFORMATION SPACE See INFORMATION ENVIRONMENT.

INFORMATION SUPPRESSION The deliberate and often systematic restriction, distortion, or concealment of politically significant information by state or non-state actors. In the context of digital media, this is frequently enacted through platforms and algorithms to influence public opinion, suppress dissent, or maintain existing power structures. Common methods include CENSORSHIP, DISINFORMATION, algorithmic downranking, biased content moderation, and internet shutdowns.

INFORMATION WARFARE A term that is: [1] used interchangeably with INFORMATION OPERATIONS; [2] used as a key component of various modes of warfare waged below the level of direct military confrontation (such as COGNITIVE WARFARE, HYBRID WARFARE, LAWFARE, POLITICAL WARFARE, PSYCHOLOGICAL WARFARE, PUBLIC OPINION WARFARE); [3] used to describe information and communication technologies-centred confrontation in the battlespace. The Russian concept of **information confrontation (**информационное противоборство, *informatsionnoye protivoborstvo*) reflects the second broad meaning listed above, as a long-term form of non-kinetic confrontation aiming at mollifying the socio-political and cultural cohesion of an adversary by operating in its INFORMATION SPACE/ENVIRONMENT, in light of hard power asymmetry. Russia's concept of **information war** (информационная война, *informatsionnaya voyna*), however, is more akin to STRATEGIC COMMUNICATIONS, as it focuses on how actions, rather than information, can enable effective communications with multiple foreign audiences to serve the state's objective. In the case of China, information war (信息战, *xinxizhan*) is either subsumed within the PSYCHOLOGICAL WARFARE and POLITICAL WARFARE paradigms, or within the battlespace-related concept of electronic warfare.

INTERFERENCE The disruption of the political, economic, and socio-cultural processes of a target actor mainly through clandestine means. In contrast with INFLUENCE, interference is not primarily concerned with shaping perceptions and behaviours of the target actor, aiming instead at rendering it dysfunctional in the context of a confrontation. COGNITIVE WARFARE, HYBRID WARFARE, INFORMATION OPERATIONS/WARFARE, LAWFARE, POLITICAL WARFARE, PSYCHOLOGICAL WARFARE, PUBLIC OPINION WARFARE, SHARP POWER, and SUBVERSION WAR can be understood as historically specific and/or geographically specific modes of interference. ACTIVE MEASURES, CYBER ATTACKS, DISINFORMATION, FAKE NEWS, KOMPROMAT, ORGANISED SOCIAL MEDIA MANIPULATION, SHARP POWER, and UNITED FRONT WORK can be understood as means for interference.

INTERNATIONAL MEDIA DEVELOPMENT A term used in China to refer to evolution and change in the fields of news media and communications. In detail, international media development concerns the development of an international presence for all of China's most prominent state-owned media outlets, and the support of journalist and media organisations who are supported by, trained by and aligned with China, especially in the Global South.

INTERNET SOVEREIGNTY (网络主权, *wangluo zhuquan*). A concept underlying the idea that the state has the right to manage and control the internet within its borders according to its own national interests, including the regulation of information and data flows. The concept informs the Chinese government enforcement of CENSORSHIP ("HARMONIZATION") strict regulations over internet usage, content, data management within the country, and stringent data localization laws that require international companies operating in China to store Chinese users' data within the country.

INTERNET SURVEILLANCE The gathering, observation, and analysis of information from online activity. The content of surveillance can include anything, from emails and social media posts, to browsing history and search terms.

"INTERNET WATER ARMY" (网络水军, *wangluo shui jun*). Paid internet commentators who post comments favourable to the Chinese government policies in an attempt to manipulate public opinion and drown out dissenting voices. Unlike overt CENSORSHIP, which removes content, the use of these commentators is subtler, aiming to sway public opinion through the appearance of grassroots support. This strategy allows the government to maintain a semblance of lively discourse while ensuring that the digital conversation aligns with its interests. This practice not only helps stabilize the domestic INFORMATION SPACE but also serves as a tool for cyber diplomacy, where these commentators engage in international forums to influence global perceptions about China.

"KOMPROMAT" (компромат, "compromising material"). A term of Soviet origins referring to information that is strategically collected and deployed to discredit, blackmail, or manipulate individuals or organizations. It includes private communications, financial records, misconduct evidence, or other sensitive details. This tactic, rooted in Soviet intelligence tactics, is used to ruin reputations, coerce compliance, or influence public opinion and political outcomes, and extends beyond Russia to international diplomacy.

LAWFARE (also known as **LEGAL WARFARE**): The use of legal tools to achieve an actor's objective either on the battlefield or in a politico-diplomatic competition. Lawfare emerged in the U.S. in the contest of the Global War on Terror with the aim to support and demonstrate the "legality" of kinetic operations in the battlefield. The concept emerged in China between the late 1990s and the early 2000s. In China, lawfare is one of the THREE WARFARES, together with PSYCHOLOGICAL WARFARE and PUBLIC OPINION WARFARE. Chinese lawfare is primarily concerned with the use of legal tools in politico-diplomatic contests as a result of the country's maritime and territorial disputes. The instrumental conceptions of international law, traceable to Soviet Marxism-Leninism legal theories, further inform Beijing's own distinct use of legal tools.

MISINFORMATION The act of inadvertently sharing DISINFORMATION, FAKE NEWS, and other forms of partially or fully erroneous or decontextualised information.

NARRATIVE COMPETITION A contestation of culturally attuned cognitive schemata among particular audiences. In this context, a narrative is a cognitive process of ordering information into a structure of cause, effect and consequence that also works as a system of stories structured in such a way as to make meaning.

NET-CENTRIC WAR A Russian conceptualisation of INFORMATION WARFARE designed to influence a network of people, instructions, foundations, organizations, that may promote a certain set of ideas to achieve certain political goals. Net-centric warfare focuses on the combat power that can be generated from the effective linking or networking of the warfighting enterprise. It is characterized by the ability of geographically dispersed forces to create a high level of shared battlespace awareness that can be exploited via self-synchronization and other network-centric operations to achieve commanders' intent.

ORGANISED SOCIAL MEDIA MANIPULATION A term describing the deliberate use of government or political party employees, often termed cyber troops, to manipulate public opinion online for political purposes. This includes disseminating both DISINFORMATION and strategically crafted truthful information to shape narratives and advance specific agendas. Additionally, organised media manipulation encompasses control over media content and channels to influence public perceptions, behaviours, and opinions, employing techniques like selective dissemination, POLITICAL ASTROTURFING, PROPAGANDA, and CENSORSHIP.

Under EC Review

PERCEPTION MANAGEMENT The intentional manipulation of information to influence how it is perceived by an audience. This involves controlling or shaping information to affect the targets' cognitive processes and change their beliefs and actions, often through de-contextualization, distortions, and INFORMATION SUPPRESSION, as well as through the employment of psychological tactics capable to affect emotional responses.

POLITICAL ASTROTURFING A top-down, coordinated DISINFORMATION effort in which actors participate to processes of political communications within the INFORMATION SPACE – generally on social media – with the aim to project genuine support for a specific electoral candidate, a political figure or a narrative. A form of SOCIAL MEDIA WARFARE and of SOCIAL NETWORK MANIPULATION.

POLITICAL WARFARE The employment of all available means by a state, short of direct military confrontation, to achieve its objectives. Political warfare encompasses the use of a very wide range of national and international instruments in efforts to persuade, intimidate, coerce, undermine, and weaken opponents, and hence achieve desired political goals. The only major activity excluded from this conception of political warfare is the use of kinetic force in an overt military confrontation with the opponent. Political warfare makes use of assertive diplomacy, INFORMATION OPERATIONS, economic statecraft, infiltration and subversion, strategic corruption, hacking and other forms of CYBERATTACKS, military signalling, and deniable deployment of military and paramilitary forces below the threshold of overt military confrontation. The concept is contiguous to HYBRID WARFARE, and to a lesser extent GREY ZONE OPERATIONS and PSYCHOLOGICAL WARFARE. When it comes to **China**, political warfare, also describes, in a narrower fashion, what is known as the "political work" (政治工作, *zhengzhi gongzuo*) of the People's Liberation Army, namely a range of operations below the threshold of direct military confrontation, including psychological operations, PROPAGANDA, and military PUBLIC DIPLOMACY. In the case of **Russia**, political warfare lacks an official conceptualisation by bureaucratic actors, and can be understood as a broad framework comprising activities conceptualised as ACTIVE MEASURES, HYBRID WARFARE, INFORMATION OPERATIONS/WARFARE, and other modes of international competition short of direct military confrontation. Russian political warfare is thus the result of a wide network of bureaucratic actors within the intelligence, security, and military services of the country, state media, state-adjacent actors (including diasporic communities and criminal groups), and foreign actors who are ideologically, tactically and/or financially linked to Russia.

Under EC Review

POST-TRUTH The erosion of shared objective standards of truth resulting in denying the existence of a verifiable independent reality. It involves muddying the waters to the extent that distinguishing between truth and falsehood becomes challenging, rather than solely pushing lies as truths.

PRECISE COMMUNICATION A concept concerning the enhancement of the international influence of China's PROPAGANDA work. Precise communication involves tailoring content dissemination methods to specific target audiences based on in-depth understanding obtained through data analysis, surveys, and behavioural data. The aim is to maximize the impact of China's narratives abroad by customizing content based on audience preferences, interests, and values, creating messages that resonate effectively with smaller constituencies and even individuals. Precise communications is influenced by advertising theories and relies on contemporary communication technologies and AI to reach target audiences more effectively. The concept is contiguous to the Chinese conceptualisation of STRATEGIC COMMUNICATIONS.

PROPAGANDA A mode of political communication consistently (but not exclusively) relying on one-way information flows and the simplification, distortion, and de-contextualisation of information to INFLUENCE perceptions, shape behaviours, and – when the actor holds political power – enforce rules among target audiences. Modern understandings of propaganda coalesced during the First World War (1914-1918). They

are however primarily associated with the authoritarian regimes of the 20th century, and especially with the totalitarian regimes of that era and their absolute control of their mass media and of the private lives of their citizens. Popular understandings of propaganda often simply equate it to DISINFORMATION. Propaganda can be categorised according to multiple criteria. [1] According to its ends ("political propaganda", "agitational propaganda", "integration propaganda", "sociological propaganda", "legal propaganda", "military propaganda"). [2] Via the identity of the propagandist, be it a state actor or a specific bureaucratic actor within a state, an insurgent or a terrorist group, a political movement or party. [3] In relation to a perceived opponent ("offensive propaganda" vs. "defensive propaganda"). [4] According to the medium chosen for the dissemination of the message ("propaganda by word", "propaganda by deeds", "audio/visual propaganda"). [5] According to a specific domain or set of tools and techniques used to create and disseminate content (cyber propaganda, computational propaganda). Contemporary perceptions of propaganda are negative at a global level following the two world wars and the experience of 20th century totalitarian regimes. Virtually all state actors refute accusations to produce and disseminate propaganda. Modes of state communications such as PUBLIC DIPLOMACY and STRATEGIC COMMUNICATIONS have been devised to avoid such accusations.
Propaganda in China (宣传, *xuanchuan*): Leninist regimes such as China refute moralistic conceptualisation of propaganda, even though they officially translate the term as "publicity" in communications with foreign actors and in foreign contexts. "Propaganda work" (宣传工作, *xuanchuan gongzuo*) remains a crucial activity essential to the exercise of political power within the country and to the projection of China's image and power abroad. Propaganda work is implemented by the country's "propaganda system" (宣传体系, *xuanchuan tixi*), a sprawling network of institutions across the party and the state, with the Propaganda Department of the CCP at its top. Propaganda work does not simply concern the control of media and communication (thus enforcing CENSORSHIP and HARMONIZATION) within the country. It also concerns public education, party education and training of state officials, ideological construction, diplomacy (being it traditional, public, economic, military, health-related, etc.), and military affairs (with the implementation of THREE WARFARES and POLITICAL WARFARE). Propaganda activity can be roughly classified as "internal" (内宣, *neixuan*) and "external" (外宣, *waixuan*), yet there is also propaganda specifically targeting oversea Chinese communities and propaganda targeting Taiwan which eschews clear-cut definitions.
Propaganda in Russia (пропаганда): Russian propaganda lacks the Leninist bureaucratic organisation of China. It has a polycentric nature, with multiple bureaucratic actors within the intelligence, security, and military services of the country involved in its creation. Its dissemination relies on state and state-adjacent media, but foreign individuals and networks aligned with Moscow play a key role in its propagation within foreign INFORMATION SPACES. Russian propaganda has been described as high-volume, multichannel, rapid, continuous, repetitive, with no commitment to objective reality and consistency.

PSYCHOLOGICAL MANIPULATION Any type of activity aimed at raising threat perceptions or intensifying popular emotions, such as anger, to elicit confrontational policy preferences. It may also seek to draw out expressions of support to amplify the state's voice or suppress dissent, generating psychological pressure on a foreign target. Wide-ranging and co-ordinated acts of psychological manipulation can be understood as PSYCHOLOGICAL WARFARE.

PSYCHOLOGICAL WARFARE A mode of confrontation designed to challenge prevailing narratives and beliefs within a target country or community, with the aim of hijacking the cognitive processes of the target and changing its thought processes and behaviours in favour of the opponent. "**Psychological operations"** is the equivalent term in the Euro-Atlantic military and security milieus. In the NATO context, psychological operations differ from STRATEGIC COMMUNICATION as they are not bound by the necessity to maintain standards of truthfulness and reflect the values of the organisation and of its member states. In China, psychological warfare (心理战, *xinlizhan*) is a key component of the THREE WARFARES. Chinese psychological warfare is primarily different from PUBLIC OPINION WARFARE because of the identity of the target: the former

Under EC Review

targets decision-maker elites, and armed forces, the latter the general public. Chinese PSYCHOLOGICAL WARFARE is also the foundation of COGNITIVE WARFARE.

PUBLIC DIPLOMACY The practice by which states communicate, interact, and engage with foreign audiences in order to influence their perceptions and opinions in a positive manner. It involves the promotion of a country's culture, values, policies, and image through transparent and credible communication. Public diplomacy emphasizes mutual understanding, cultural exchanges, and dialogue, seeking to attract and persuade rather than coerce – thus being a key tool for actualising a country's SOFT POWER. It emerged in the U.S. during the Cold War in a conscious attempt to distinguish its political communication from PROPAGANDA. Public diplomacy in **China** has been a central concept in the country's political communication since the 2000s. Yet, its conceptualisation in the country has remained vague and contradictory given the continuing existence of a Leninist PROPAGANDA system, which has remained in fact responsible for its performance. Public diplomacy in Russia has focused since the 2000s on promoting the country's cultural attractiveness while at the same time presenting it as a bulwark against U.S. hegemony, Western liberal democracy, and "globalism". Crucially, Russia's public diplomacy openly makes use of PROPAGANDA, DISINFORMATION, and more broadly INFORMATION OPERATIONS to achieve its objectives.

PUBLIC OPINION GUIDANCE (舆论引导, *yulun yindao*). A term describing the Chinese strategy of directing (primarily domestic) public discourse in a way that aligns with government policies and objectives. It emphasizes shaping the interpretation of events and information in a manner that supports national stability and unity. Public opinion guidance involves multiple layers of media CENSORSHIP, executed through state-run media outlets and stringent regulation of digital platform, specifying how certain events and topics should be reported. Key tools include content filtering, blocking of websites that offer dissenting viewpoints, and the use of internet commentators (see INTERNET WATER ARMY and TROLLS) who post pro-government comments to influence discussions online. Public opinion guidance does not simply concern the dissemination and censorship of information but also the management of nationalist protests in case of international dispute.

PUBLIC OPINION WARFARE One of the components of the THREE WARFARES. Public opinion warfares aims to shape and manipulate public opinion within an adversary to undermine its internal cohesion during a confrontation or open conflict.

SHARP POWER A mode of authoritarian influence targeting liberal democracies conceptualised in Western policy and academia environments. Sharp power aims at obtaining the same outcomes of SOFT POWER by mixing tools generally associated with the latter, such as people-to-people exchanges, cultural activities, educational programs, and media enterprises, with bullying or coercive tactics.

SOCIAL ENGINEERING The manipulation of individuals or groups to divulge confidential information or perform actions that are not in their best interest, but which serve the manipulator's purpose. This is achieved through deceptive interactions that exploit human psychological vulnerabilities, such as trust, fear, or the desire to be helpful, often through personalised approaches based on detailed knowledge of the victims.

SOCIAL MEDIA WARFARE A medium-focused term used to describe forms of INFORMATION WARFARE, POLITICAL WARFARE, PSYCHOLOGICAL WARFARE, PUBLIC OPINION WARFARE, in which social media are used as a weapon with the aim of causing lasting damage to certain actors such as governments or companies.

SOCIAL NETWORK MANIPULATION The use of government or political party employees or contractors, often called cyber troops, to manipulate public opinion online for political purposes across multiple social media platforms. See: "INTERNET WATER ARMY", TROLLS.

Under EC Review

SOFT POWER The intentional projection by a state of a specific self-identity with the aim of exerting influence beyond its national borders through non-coercive means. A concept that emerged in Western academia between the 1990s and the 2000s. It involves leveraging cultural attractiveness, diplomatic initiatives, and image laundering strategies to shape the perceptions and beliefs of foreign populations about the sponsoring government. This concept is often associated with efforts to cultivate positive impressions and affiliations with a nation's values, culture, and policies in order to garner support or sway opinions abroad. However, the effectiveness of soft power initiatives may vary depending on factors such as the familiarity of the target population with the sponsoring government and the existing perceptions of its actions and policies.
Soft power in China has been embraced by party and state institutions since the late 2000s. In the Chinese discourse, soft power is closely linked to "cultural power" and to DISCOURSE POWER. Chinese soft power is therefore characterised by a top-down pro-active approach by party and state institutions, rather than by bottom-up dynamics, thus also being closely linked to PUBLIC DIPLOMACY. Cultural attractiveness is central in the Chinese construction of soft power, in contrast to the original conceptualisation in the West, which sees culture as one of several dimensions. Mega-events, as well as cultural exhibitions and exchanges are seen as key soft power tools.
Soft power in Russia has also been embraced by the Russian state since the late 2000s and similarly conceptualised as a form of cultural power to gain and use to resist Western hegemony. Russian soft power targets several "niche" audiences across the world and across the political spectrum and is articulated both in centralised and a decentralised fashion.

STRATEGIC COMMUNICATIONS The use of words, actions, images, or symbols to influence audiences and shape their behaviour in order to advance interests and policies and achieve objectives. Western actors such as NATO and the EU inextricably tie their conceptions of strategic communications not only to interests but also to (liberal and democratic) political values. Original conceptions of strategic communications emerged from the US-NATO milieus during the Global War on Terror and the interventions in Afghanistan and focused on the dissemination of coordinated and coherent messaging across different channels to achieve political objectives. In the case of Russia, strategic communications is conceptualised as INFORMATION WAR (информационная война, *informatsionnaya voyna*), as it focused on how actions, rather than information, can enable effective communications with multiple foreign audiences to serve the state's objective. In the case of China, the term strategic communications (战略传播, *zhanlüe chuanbo*), has been used to discuss a wide range of issues on the effectiveness, adaptiveness, and localisation of PROPAGANDA targeting foreign actors.

STRATEGIC NARRATIVES Narratives that are crafted and disseminated with the specific aim to contribute to the realization of a goal by affecting the cognitive process of their targets. In NATO understanding of STRATEGIC COMMUNICATIONS, all narratives are conceived as inherently strategic, thus the term is not used.

SUBVERSION WAR A Russian conceptualization of war which involves exploiting existing domestic turmoil for political gain, whether through direct or indirect means, amidst rapid political, social, and cultural transformations.

THOUGHT WORK (思想工作, *sixiang gongzuo*). The efforts to educate and indoctrinate the public and party members with the values and principles considered correct by the Chinese Communist Party, often through controlled information channels. Thought Work extends to the internal discipline of the party, where party members are regularly required to attend study sessions and ideological training to maintain their commitment to the principles of the party and to prevent the infiltration of corrupt or "foreign" ideas. The implementation of Thought Work is not merely about disseminating information but involves active dialogue, feedback mechanisms, and the adjustment of strategies based on public reception and internal party

Under EC Review

dynamics. It is a dynamic and ongoing process that adapts to new challenges and opportunities to reinforce the party's legitimacy and authority.

THREE WARFARES (三战, *sanzhan*). A People's Liberation Army's concept that focuses on the combination of PSYCHOLOGICAL WARFARE, PUBLIC OPINION WARFARE, and LAWFARE to advance a country's interests and objectives. The Three Warfares can be waged, within and outside the battlefield, and exist both at a strategic level, at an operational level, and at a tactical level. Cross-domain, and therefore HYBRID in nature, each of the Three Warfares is waged first and foremost in the information domain.

"TROLL" An individual who frequently chooses to remain anonymous while engaging in online activities aimed at persuading or influencing others' thoughts and emotions. Trolls often utilize deceptive or half-truthful information in their posts, with the intention of steering conversations or shaping opinions on various online platforms. Organized operations employing trolls to work in a coordinated fashion to manipulate public discourse by disseminating or contrasting certain narratives, are called **troll farms**. Both China ("50 Cent Party", 五毛党, *wumaodang*) and Russia (Internet Research Agency) are known to have made use of troll farms.

UNITED FRONT WORK (统一战线工作, *tongyi zhanxian gongzuo*). A set of overt and covert practices of Leninist origins aimed at fostering, maintaining, and mobilising networks of allies and friends among foreign and oversea Chinese communities aimed at supporting the Party in contested environments. United front Work is undertaken by a system of Party, State, and Party-State adjacent organisations, ultimately coordinated by the United Front Work Department. UFW activities may involve "elite capture" through strategic corruption, co-optation, and initiatives of lobbying. It is a critical component of China's POLITICAL WARFARE. Hong Kong, Macau, and Taiwan have long been key loci of united front work operations, but throughout the 2010s, they also considerably expanded abroad. The academe, former political officials, as well as media figures are traditional united front work targets.

UNRESTRICTED WARFARE (aka "beyond-boundaries-warfare", 超限战, *chaoxianzhan*). A Chinese conceptualisation of warfare based on transcending boundaries between battle-domains and between traditional understanding of "wartime" and "peacetime" activities. A precursor of the THREE WARFARES, and a concept contiguous to HYBRID WARFARE.

Under EC Review

APPENDIX

Sources consulted for the compilation of this glossary.

Alpermann, Björn, and Michael Malzer. "“In Other News”: China's International Media Strategy on Xinjiang—CGTN and New China TV on YouTube." *Modern China* 50, no. 2 (2024): 135-178.

Andrzejewski, Catherine. *Innovators and Emulators. China and Russia's Compounding Influence on Digital Censorship*. International Republican Institute, 2023.

Babbage, Ross. *Winning Without Fighting: Chinese and Russian Political Warfare Campaigns and How the West Can Prevail.* CSBA, 2019.

Bachman, Elizabeth, and James Bellacqua. *Black and White and Red All Over: China's Improving Foreign-Directed Media*. CNA, 2020.

Baggott Carter, Erin, and Brett L. Carter. "Questioning More: RT, Outward-Facing Propaganda, and the Post-West World Order", *Security Studies* 30, no. 1 (2021): 49-78.

Baughman, Josh. *How China Wins the Cognitive Domain*. CASI, 2023.

Beauchamp-Mustafaga Nathan, and Andew Chase. *Borrowing a Boat Out to Sea: The Chinese Military's Use of Social Media for Influence Operations*. SAIS, 2019.

Beauchamp-Mustafaga, Nathan. "Cognitive Domain Operations. The PLA's New Holistic Concept for Influence Operations." *China Brief* 19, no. 16 (2019), unpaginated.

——. *Chinese Next-Generation Psychological Warfare: The Military Application of Emerging Technologies and Implications for the United States*. RAND, 2023.

Bennett, W. Lance, and Alexandra Segerberg. *The Logic of Connective Action: Digital Media and the Personalization of Contentious Politics.* Cambridge: Cambridge University Press, 2013

Bērziņa Čerenkova, Una Aleksandra, et al. *China's Influence in the Nordic-Baltic Information Environment: Latvia and Sweden*. NATO Strategic Communications CoE, 2022.

Bolsover, Gillian. "Computational Propaganda in China. An Alternative Model of a Widespread Practice." *Computational Propaganda Working Papers 4* (2017).

Bodnar, Joseph, Etienne Soula, and Brent Schafer. *A Year of Disinformation: Russia and China's Influence Campaigns During the War in Ukraine*. German Marshall Fund, 2023.

Brady, Anne-Marie. "China's Foreign Propaganda Machine." *Journal of Democracy* 26, no. 4 (2015): 51-59.

——. "Guiding Hand. The Role of the CCP Central Propaganda Department in the Current Era." *Westminster Papers in Communications and Culture* 3, no. 1 (2017).

——. *Magic Weapons: China's Political Influence Activities under Xi Jinping.* Wilson Center, 2017.

——. "Exploit Every Rift. United Front Work Goes Global." *Party Watch Annual Report 2018*. Center for Advanced China Research, 2018.

Under EC Review

Charon, Paul, and Jean-Baptiste Jeangène Vilmer. *Chinese Influence Operations: A Machiavellian Moment*. IRSEM, 2021.

Chen, Ketty W., and J. Michael Cole. *CCP and Proxy Disinformation: Means, Practices, and Impact on Democracies*. Sinopsis, 2019.

Cheng, Dean. *Winning Without Fighting: Chinese Legal Warfare*. The Heritage Foundation, 2012.

Chubb, Andrew, and Frances Yaping Wang. "Authoritarian Propaganda Campaigns on Foreign Affairs: Four Birds, One Stone, and the South China Sea Arbitration." *International Studies Quarterly* 67, no. 3 (2023): 1-15.

Chung, Youngjune. "Allusion, Reasoning and Luring in Chinese Psychological Warfare." *International Affairs* 97, no. 4 (2021): 1007-1023.

Chung, Youngjune. "Hybrid Challenges in the PRC's Novel Public Opinion Warfare." *Pacific Focus* 36, no. 3 (2021): 405-426.

Clack, Timothy, and Johnson, Robert. *The World Information War Western Resilience, Campaigning, and Cognitive Effects*. Routledge, 2021.

Colley, Thomas, and Martin Moore. "News as Geopolitics: China, CGTN and the 2020 US Presidential Election." *The Journal of International Communication* 29, no. 1 (2023): 82-103.

Cook, Sarah. *Beijing's Global Megaphone: The Expansion of CCP Media Influence since 2017*. Freedom House, 2020.

Creemers, Rogier. "Never the Twain Shall Meet. Rethinking China's Public Diplomacy Policy." *Chinese Journal of Communication* 8, no. 3 (2015): 306-322.

——. "Cyber China: Upgrading Propaganda, Public Opinion Work and Social Management for the Twenty-First Century." *Journal of Contemporary China* 26, no. 103 (2017): 85-100.

Deal, Jacqueline N. "Information Warfare: Disintegrating the Enemy: The PLA's Info-Messaging." *Parameters* 50, no. 3 (2020): 5-16.

DFRLab. *Chinese Discourse Power: China's Use of Information Manipulation in Regional and Global Competition.* Atlantic Council, 2020.

Dov Bachmann, Sascha-Dominik, Dries Putter, and Guy Duczynski. "Hybrid Warfare and Disinformation: A Ukraine War Perspective." *Global Policy* 14, no. 5 (2023): 858-869.

Doxsee, Catrina, Emily Harding, and Seth Jones. *Competing Without Fighting: China's Strategy of Political Warfare*. CSIS, 2023.

Drinhausen, Katja, et al. *Image Control. How China Struggles for Discourse Power.* MERICS, 2023.

Edney, Kingsley. *The Globalization of Chinese Propaganda: International Power and Domestic Political Cohesion*. Palgrave, 2014.

Under EC Review

Fabian, Sandor. "The Russian hybrid warfare strategy – neither Russian nor strategy." *Defense & Security Analysis* 35, no. 3 (2019): 308-325.

Fan, Yingjie, Jennifer Pan and Jaymee Sheng. "Strategies of Chinese State Media on Twitter." *Political Communication* 41, no. 1, (2024): 4-25.

Farwell, James P. *Power and Persuasion: The Art of Strategic Communication*. Georgetown University Press, 2012.
Hicks, Kathleen, and Alice Hunt Friend, eds. *By Other Means: Campaigning in the Gray Zone*. CSIS, 2019.

Fedor, Julie. "Spinning Russia's 21st Century Wars: Zakhar Prilepin and his 'Literary Spetsnaz'". *The RUSI Journal*, 163, no. 6 (2018): 18-27.

Fridman, Ofer. "Hybrid Warfare or Gibridnaya Voyna? Similar But Different." *The RUSI Journal*. 162, no.1 (2017): 42-49.

——. "The Russian Perspective on Information Warfare: Conceptual Roots and Politicisation in Russian Academic, Political, and Public Discourse." *Defence Strategic Communications* 2 (2017): 61-86.

——. *Russian "Hybrid Warfare": Resurgence and Politicization*. Oxford University Press, 2019.

——. "'Information War' as the Russian Conceptualisation of Strategic Communications", *The RUSI Journal* 165, no. 1 (2020): 44-53.

——. "Inherent Strategic Ambiguity between Objectives and Actions: Russia's 'Information War'". *Defence Strategic Communications*,*12* (2023): 187-230.

Friedman, Toni. *Lexicon: 'Discourse Power' or the 'Right to Speak'*. DigiChina, 2022.

Galeotti, Mark. "Hybrid, Ambiguous, and Non-Linear? How New Is Russia's 'New Way of War'?," *Small Wars & Insurgencies* 27, no. 2 (2016): 282-301.

——. *Controlling Chaos: How Russia Manages Political Warfare in Europe.* ECFR, 2017.

——. *Russian Political War. Moving Beyond the Hybrid*. Routledge, 2019.

——. *The Weaponisation of Everything: A Field Guide to the New Way of War*. Yale University Press, 2022.

Gallacher, John D., and Marc W. Heerdink. "Measuring the Effect of Russian Internet Research Agency Information Operations in Online Conversations." *Defence Strategic Communications* 6 (2019): 155-198.

Gamso, Jonas. "Is China Exporting Media Censorship？China's Rise, Media Freedoms, and Democracy." *European Journal of International Relations* 27, no. 3 (2021): 858-883.

Gershaneck, Kerry K. "Political Warfare: The People's Republic of China's Strategy 'To Win without Fighting'." *Journal of Advanced Military Studies* 11, no. 1 (2020): 64-93.

Gillespie, Tarleton. *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*. Yale University Press, 2018

Under EC Review

Hackenesch, Christine, and Julia Bader. “The Struggle for Minds and Influence: The Chinese Communist Party’s Global Outreach.” *International Studies Quarterly* 64, no. 3 (2020): 723-733.

Halper, Stefan. *China: The Three Warfares*. U.S. Department of Defense, 2013.

Hamilton, Clive, and Mareike Ohlberg. *The Party Speaks for You: Foreign Interference and the Chinese Communist Party’s United Front System*. ASPI, 2020.

Harold, Scott W., et al. *Chinese Disinformation Efforts on Social Media*. RAND, 2021.

Hartig, Falk. *Chinese Public Diplomacy: The Rise of the Confucius Institute*. Routledge, 2015.

——. “How China Understands Public Diplomacy. The Importance of National Image for National Interests.” *International Studies Review* 18, no. 4 (2016): 655-680.

Hasen, Richard L. *Cheap Speech: How Disinformation Poisons Our Politics – and How to Cure It*. Yale University Press, 2022.

Helmus, Todd C., et al. *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe*. RAND, 2018.

Hoffman, Samantha. *Engineering Global Consent. The Chinese Communist Party’s Data-Driven Power Expansion*. ASPI, 2019.

Holz, Heidi and Anthony Miller. *China’s Playbook for Shaping the Global Media Environment*. CNA, 2020.

Howard, Philip N. *Lie Machines: How to Save Democracy from Troll Armies, Deceitful Robots, Junk News Operations, and Political Operatives*. Yale University Press, 2020.

Howard, Philip N., and Muzammil M. Hussain. *Democracy’s Fourth Wave? Digital Media and the Arab Spring.* Oxford: Oxford University Press, 2013

Huovinen, Petri. *Hybrid Warfare: Just a Twist of Compound Warfare? Views on Warfare from the United States Armed Forces Perspective*. National Defense University, 2011.

Insikt Group. *1 Key for 1 Lock: The Chinese Communist Party's Strategy for Targeted Propaganda*. Recorded Future, 2022.

Insisa, Aurelio. “China’s Discourse on Strategic Communications: Insight’s into PRC External Propaganda.” *Defence Strategic Communications* 10 (2022): 111-152.

——. “Hybrid After All: The “Grey Zone”, the Hybrid Warfare Debate, and the PLA’s Science of Military Strategy.” *Defence Strategic Communications* 12 (2023): 165-186.

Jackson, Dan. *Distinguishing Disinformation from Propaganda, Misinformation, and ‘Fake News’*. International Forum for Democratic Studies, 2017.

Jankowicz, Nina. *How To Lose the Information War: Russia, Fake News, and the Future of Conflict.* I.B. Tauris, 2020.

Under EC Review

Jirouš, Filip, and Petra Ševčíková. *Covert Propaganda Operations in Plain Sight: The CCP United Front System's Media Network in Europe*. Sinopsis, 2021.

Johnson, Blake et al. *Suppressing the Truth and Spreading Lies: How the CCP Is influencing Solomon Is' Information Environment*. ASPI, 2022.

Juurvee, Ivo, et al. *Russia's Footprint in the Nordic-Baltic Information Environment 2019/2020*. NATO Strategic Communications CoE, 2021.

Kania, Elsa. *The Right to Speak: Discourse and Chinese Power*. Center for Advanced China Research, 2018.

——. "The PLA's Latest Strategic Thinking on the Three Warfares." *China Brief* 16, no. 13 (2016), unpaginated.

Keller, Franziska B., et al. "Political Astroturfing on Twitter: How to Coordinate a Disinformation Campaign." *Political Communication* 37, no. 2 (2020): 256-280.

Kelly, Allan, and Christopher Paul. *Decoding Crimea: Pinpointing the Influence Strategies of Modern Information Warfare*. NATO Strategic Communications CoE, 2020.

King, Gary, Jennifer Pan, and Margaret E. Roberts. "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, not Engaged Argument." *American Political Science Review* 111, no. 3 (2017): 484-501.

Kiseleva, Yulia. "Russia's Soft Power Discourse: Identity, Status and the Attraction of Power." *Politics* 35, no. 3-4 (2015): 316-329.

Kondratov, Eugene, and Elisabeth Johansson-Nogués. "Russia's Hybrid Interference Campaigns in France, Germany and the UK: A Challenge against Trust in Liberal Democracies?" *Geopolitics* 28, no. 5 (2023): 2169-2199.

Kriel, Charles, and Alexa Pavliuc. "Reverse Engineering Russian Internet Research Agency Tactics through Network Analysis." *Defence Strategic Communications* 6 (2019): 190-227.

Laruelle, Marlène. "Russia's Niche Soft Power: Sources, Targets and Channels of Influence" *Russie.Nei.Visions* 122 (2021).

Lee, Sangkuk. "China's 'Three Warfares': Origins, Applications, and Organizations." *Journal of Strategic Studies* 37, no. 2 (2014): 198-221.

Lemke, Tobias, and Michael W. Habegger. "Foreign Interference and Social Media Networks: A Relational Approach to Studying Contemporary Russian Disinformation." *Journal of Global Security Studies* 7, no. 2 (2022), unpaginated.

Lidberg, Johan, Louisa Lim, and Erin Bradshaw. "The World According to China: Capturing and Analysing the Global Media Influence Strategies of a Superpower." *Pacific Journalism Review* 29, no. 1-2 (2023): 182-204.

Lilly, Bilyana. *Russian Information Warfare. Assault on Democracies in the Cyber Wild West.* Naval Institute Press, 2022.

Under EC Review

Liu, Chuyu, and Xiao Ma. "Popular Threats and Nationalistic Propaganda: Political Logic of China's Patriotic Campaign." *Security Studies* 27, no. 4 (2018): 633-664.

Mahnken, Thomas G., Ross Babbage, and Toshi Yoshihara. *Countering Comprehensive Coercion: Competitive Strategies against Authoritarian Political Warfare*. CSBA, 2018.

Marcellino, William, et al. *The Rise of Generative AI and the Coming Era of Social Media Manipulation 3.0: Next-Generation Chinese Astroturfing and Coping with Ubiquitous AI*. RAND, 2023.

Matthews, Miriam, et al. *Understanding and Defending Against Russia's Malign and Subversive Information Efforts in Europe*. RAND, 2021.

Min, Bumgi, and Luwei Rose Luqiu. "How Propaganda Techniques Leverage Their Advantages: A Cross-national Study of the Effects of Chinese International Propaganda on the U.S. and South Korean Audiences." *Political Communication* 38, no. 3 (2020): 303-325.

Miskimmon, Alister, Ben O'Loughlin and Laura Roselle. *Strategic Narratives: Communication Power and the New World Order*. Routledge, 2013.

Mochtak, Michal, and Richard Q. Turcsanyi. "Studying Chinese Foreign Policy Narratives: Introducing the Ministry of Foreign Affairs Press Conferences Corpus." *Journal of Chinese Political Science* 26, no. 4 (2021): 743-761.

Mokry, Sabine. "China's Foreign Policy Rhetoric: Between Orchestration and Cacophony." *The Pacific Review* 37, no. 2 (2024): 360-387.

Molter, Vanessa, and Renee Di Resta. "Pandemics & Propaganda: How Chinese State Media Creates and Propagates CCP Coronavirus Narratives." *Harvard Kennedy School Misinformation Review* 1 (2020): 1-24.

Morozov, Evgeny. *The Net Delusion: The Dark Side of Internet Freedom.* New York: PublicAffairs, 2011

Naím, Moisés. *The Revenge of Power: How Autocrats Are Reinventing Politics for the 21st Century*. St. Martin's Press, 2022.

Nimmo, Ben, Ira Hubert and Yang Cheng. *Spamouflage Breakout: Chinese Spam Network Finally Starts to Gain Some Traction*. Graphika, 2021.

Nimmo, Ben, et al. *Spamouflage Goes to America: Pro-Chinese Inauthentic Network Debuts English-Language Videos*. Graphika, 2020.

Nimmo, Ben. *Combating Disinformation with the Four "Ds"*. The Center of Academic Innovation, University of Michigan, 2020.

O'Connor, Cailin, and James Owen. *The Misinformation Age: How False Beliefs Spread*. Yale University Press, 2018.

Oud, Malin, and Katja Drinhausen (eds.) *Decoding China Dictionary*. 2023.

Paul, Christopher, and Miriam Matthews. *The Russian "Firehose of Falsehoods" Propaganda Model: Why It Might Work and Options to Counter It*. RAND, 2014.

Under EC Review

Qiang, Xiao. "Liberation Tehcnology: The Battle for the Chinese Internet." *Journal of Democracy* 22, no. 2 (2011): 47-61.

Radnitz, Scott. "Solidarity through Cynicism? The Influence of Russian Conspiracy Narratives Abroad." *International Studies Quarterly* 66, no. 2 (2022).

Repnikova, Maria. "China's Propaganda on the War in Ukraine." *China Leadership Monitor* 72 (2022),

Repnikova, Maria. "Rethinking China's Soft Power: 'Pragmatic Enticement' of Confucius Institutes in Ethiopia." *The China Quarterly* 250 (2022): 440-463.

——. *China-Russia Convergence in the Communication Sphere: Exploring the Growing Information Nexus*. Wilson Center, 2022.

Rid, Thomas. *Active Measures: The Secret History of Disinformation and Political Warfare*. Farrar, Straus and Giroux, 2020.

Ryan, Fergus, et al. *#StopXinjiangRumors: The CCP's Decentralised Disinformation Campaign*. ASPI, 2021.

Ryan, Fergus, Daria Impiombato, and Hsi-ting Pai. *Frontier Influencers: The New Face of China's Propaganda*. ASPI, 2022.

Roberts, Sarah T. *Behind the Screen: Content Moderation in the Shadows of Social Media*. Yale University Press, 2019.

Schrader, Matt. *Friends and Enemies: A Framework for Understanding Chinese Political Interference in Democratic Countries*. German Marshall Fund, 2020.

Shambaugh, David. "China's External Propaganda Work: Missions, Messengers, Mediums." *Party Watch Annual Report 2018*. Center for Advanced China Research, 2018.

Sloss, David. *Tyrants on Twitter: Protecting Democracies from Information Warfare*. Stanford University Press, 2022.

Stokes, Mark. *The PLA General Staff Department Third Department Second Bureau: Organizational Overview of Unit 61398*. Project 2049, 2015.

Stengel, Richard. *Information Wars: How We Lost the Global Battle against Disinformation and What We Can Do About It*. Grove Press, 2019.

Suchkov, Maxim A. "Whose Hybrid Warfare? How 'the Hybrid Warfare' Concept Shapes Russian Discourse, Military, and Political Practice." *Small Wars & Insurgencies* 32, no. 3 (2021): 415-440.

Szostek. Joanna. "Defence and Promotion of Desired State Identity in Russia's Strategic Narrative." *Geopolitics* 22, no. 3 (2017): 571-593.

Tan, Valarie. *Westernized' Patriots Defend China's Model*. MERICS, 2022.

Under EC Review

Thibaut, Kenton. *Chinese Discourse Power: Aspirations, Reality, and Ambitions in the Digital Domain*. Atlantic Council, 2022.

Thomas, Timothy. "Russia's 21st Century Information War: Working to Undermine and Destabilize Populations." *Defence Strategic Communications* 1 (2016): 16-25.

Treyger, Elina, Joe Cheravitch, Joe and Raphael S. Cohen. *Russian Disinformation Efforts on Social Media*. RAND, 2022.

Tufekci, Zeynep. "Algorithmic Harms Beyond Facebook and Google: Emergent Challenges of Computational Agency." Colorado Technology Law Journal, vol. 13, no. 203, 2015, pp. 203–218.

Turcsányi, Richard Q., Jan Daniel and Vojtěch Bahenský. *Dragon's Roar and Bear's Howl. Convergence in Sino-Russian Information Operations in NATO Countries*. NATO Strategic Communications CoE, 2022.

Wallis, Jacob, Albert Zhang, and Ariel Bogle. *Trigger Warning: The CCP's Coordinated Information Effort to Discredit the BBC*. ASPI, 2021.

Wang, Clyde Yicheng. "Changing Strategies and Mixed Agendas: Contradiction and Fragmentation within China's External Propaganda." *Journal of Contemporary China* 32, no. 142 (2023): 586-601,

Wang, Frances Yaping. "Barking Without Biting. Understanding Chinese Media Campaigns During Foreign Policy Disputes." *Security Studies* 30, no. 4 (2021): 517-549.

Weiss, Jessica Chen, and Allen Dafoe. "Authoritarian Audiences, Rhetoric, and Propaganda in International Crises. Evidence from China." *International Studies Quarterly* 63, no. 4 (2019): 963–973.

Weissmann, Mikael, et al. *Hybrid Warfare: Security and Asymmetric Conflict in International Relations*. I.B. Tauris, 2021.

West, Michael J., and Aurelio Insisa. "Re-Unifying Taiwan with China through Lawfare." *The China Quarterly* 257 (2024): 186-201.

Wiggell, Mikael. "Hybrid Interference as a Wedge Strategy: A Theory of External Interference in Liberal Democracy". *International Affairs* 95, no. 2 (2019): 255-275.

Xia, Shouzhi, Huang Huang and Dong Zhang. "Framing as an Information Control Strategy in Times of Crisis." *Journal of East Asian Studies* 22, no. 2 (2022): 255-279.

Yablokov, Ilya. "Conspiracy Theories as a Russian Public Diplomacy Tool: The Case of Russia Today (RT)". *Politics* 35, no. 3-4 (2015): 301-315.

Yamaguchi, Shinji, Yatsuzuka Masaaki and Momma Rira. *China's Quest for Control of the Cognitive Domain and Gray Zone Situations*. NIDS, 2023.

Yau, Niva, et al. *Countering China's Information Manipulation in the Indo-Pacific and Kazakhstan: A Framework for Understanding and Action*. International Republican Institute, 2023.

Yang, Yi Edward. "China's Strategic Narratives in Global Governance Reform under Xi Jinping." *Journal of Contemporary China* 30, no. 128 (2021): 219-233.

Under EC Review

Yoshihara, Toshi. *Chinese Information Warfare: A Phantom Menace or Emerging Threat?* USWAC, 2001.

Yoshihara, Toshi. "Evaluating the Logic and Methods of China's United Front Work." *Orbis* 64, no. 2 (2020): 230-248.

Zhang, Albert, Jacob Wallis, and Zoe Meers. *Strange Bedfellows on Xinjiang: The CCP, Fringe Media and US Social Media Platforms*. ASPI, 2021.

Zhao, Alexandre Huang, and Rui Wang. "Building a Network to 'Tell China Stories Well': Diplomatic Communication Strategies on Twitter." *International Journal of Communication* 13 (2019): 2984-3007.

Zhao, Kejin. "China's Rise and Its Discursive Power Strategy." *Chinese Political Science Review* 1, no. 1 (2016): 539-564.

Under EC Review

GA 101132671

info@deconspirator-project.eu

www.deconspirator-project.eu

Under EC Review

Partners