The Convergence of Disinformation: Examining Russia and China's Partnership in the Digital Age

Edited by
Niklas Swanström
and
Filip Borges Månsson

Special Paper | December 2024

Institute for Security & Development Policy

The Convergence of Disinformation: Examining Russia and China's Partnership in the Digital Age

Edited by

Niklas Swanström

and

Filip Borges Månsson

Special Paper

December 2024

Institute for Security & Development Policy

"The Convergence of Disinformation: Examining Russia and China's Partnership in the Digital Age" is a Special Paper published by the Institute for Security and Development Policy. The Institute is based in Stockholm, Sweden, and cooperates closely with research centers worldwide. The Institute serves a large and diverse community of analysts, scholars, policy-watchers, business leaders, and journalists. It is at the forefront of research on issues of conflict, security, and development. Through its applied research, publications, research cooperation, public lectures, and seminars, it functions as a focal point for academic, policy, and public discussion.

ISBN: 978-91-88551-61-0

Distributed in Europe by:

Institute for Security and Development Policy
Västra Finnbodavägen 2, 131 30 Stockholm-Nacka, Sweden
Tel. +46-841056953; Fax. +46-86403370
Email: info@isdp.eu

Editorial correspondence should be directed to the address provided above (preferably by email).

Cover Photo: Haris Mm / Shutterstock

Contents

List of Contributors

Dr. Niklas Swanström is the Director of the Institute for Security and Development Policy, and one of its co-founders. He is a Fellow at the Foreign Policy Institute of the Paul H. Nitze School of Advanced International Studies (SAIS) and a Senior Associate Research Fellow at the Italian Institute for International Political Studies (ISPI). His main areas of expertise are conflict prevention, conflict management and regional cooperation; Chinese foreign policy and security in Northeast Asia; the Belt and Road Initiative, traditional and non-traditional security threats and its effect on regional and national security as well as negotiations. His focus is mainly on Northeast Asia, Central Asia and Southeast Asia. Dr. Swanström has authored, co-authored or edited a number of books, including: Eurasia's ascent in Energy and geopolitics; Sino-Japanese Relations: The Need for Conflict Prevention and Management; Transnationell brottslighet: ett säkerhetshot? (Trans-national Crime: A Security Threat?); Regional Cooperation and Conflict Management: Lessons from the Pacific Rim; and Foreign Devils, Dictatorship or Institutional Control: China's foreign policy towards Southeast Asia.

Filip Borges Månsson is the Executive Assistant at the Institute for Security & Development Policy. He holds a Bachelor of Arts (BA) in Political Science with a minor in History from Stockholm University. Mr. Borges Månsson is a former exchange student at the University of Warsaw where he did Security and Foreign Policy Studies. Additionally, Mr. Borges Månsson has studied Intelligence Operations and Threat & Risk Management at the Swedish Defence University throughout his tenure at ISDP as EA. Mr. Borges Månsson was a co-author of "Taiwan-PRC Crisis: What Cross-Strait Conflict Could Cost Europe", and has during his internship at the Stockholm Center for South Asian and Indo Pacific Affairs (SCSA-IPA) written "Sweden's Quest for a Foothold in India's Defense Market", as well as co-authored several volumes of the "India Sweden Strategic Compass" newsletter.

Wen Cheng Fu, is a professor and department head in the Department of Journalism, the National Defense University Taiwan. He received his Ph.D. in College of Media, the University of Illinois at Urbana Champaign (UIUC). His research fields include cognitive warfare, public opinion, and data science, especially national security and military issues.

Wen Jian Huang is a naval officer in Taiwan's Ministry of National Defense, has conducted research and worked on political communication, countering disinformation, and information warfare.

Marek Kohv is the Head of Security & Resilience Programme at the ICDS with a 20-year security and national defense background. He has filled many positions in the public service including lastly as the Head of Analysis at the Government Office's National Security and Defense Coordination Bureau. Marek Kohv has also served in the Defense Forces, including various positions in the Military Intelligence Centre and Joint Headquarters of the Estonian Defense Forces. He holds a master's degree in European Union and International Law from Tallinn University of Technology.

Johan Wiktorin has more than 25 years of active military service, where his last assignment was as acting Head of R&D in the Swedish Military and Security Directorate. He led a team at PwC Sweden during the general election 2018, where they disclosed in public a disinformation online campaign, targeting Arabic-speaking residents against the Center-right party Moderaterna, which was orchestrated from the Middle East. In 2019, he co-founded Intil Group, which develops Executive Intelligence for its clients in the private sector and has authored several tailored reports to clients to uncover malign disinformation against them. He is an elected fellow of the Royal Academy of War Sciences since 2007 and is currently leading the Academy's 3-year project on how to deter Hybrid warfare.

Ilan Berman is Senior Vice President of the American Foreign Policy Council in Washington, DC, and director of the Council's Future of Public Diplomacy Project.

Dr. Shiaushyang Liou (劉蕭翔) is an Associate Research Fellow of the National Security Studies Division at the Institute for National Defense and Security Research (INDSR) and an Adjunct Assistant Professor of the Department of Diplomacy at National Chengchi University (NCCU) in the Republic of China (Taiwan). He is also an associated senior research fellow at the Institute for Security and Development Policy (ISDP) in Sweden. His research focuses on Security Studies, Russian and Eurasian Studies, Arctic Geopolitics, and China's "One Belt One Road" initiative.

Jeanette Serritzlev is a Military Analyst at the Royal Danish Defense College and holds a Master of Arts in Communications and a Master of Military Studies. Her specialization and expertise is on information warfare and hybrid threats, especially in relation to Russia. She is the author of the Danish book "Information Warfare – Influence & propaganda in Modern Warfare (2023).

Anna Rennéus Guthrie is the Director of the think-tank Stockholm Free World Forum. Anna has a background in journalism, opinion making and the Swedish business sector. Since 2007 Anna has worked for various Swedish news and media outlets as well as more than a decade for Sweden's largest employer organization. Educated at Edinburgh University (Religious Studies/History), Stockholm University (BA Literature, Master thesis English Literature) Södertörn University (International Master's Programme Journalism) as well as additional education for professionals at the Swedish Defense University.

Shih-Hung Lo holds a Ph.D. from the London School of Economics and is currently a professor in the Department of Communication at National Chung Cheng University in Taiwan. He also serves as the Chairman of the Taiwan FactCheck Education Foundation. His areas of expertise include political economy of communication, communication policy, and Chinese media studies.

Eve Chiu works as the CEO and Editor-in-chief of Taiwan Fact Check Center (TFC). With a doctoral degree in communication, she is a researcher of communication history and a veteran, award-winning journalist. In her media-related career, Chiu has provided invaluable insights to Taiwanese government departments and media industry alike. She was on the Board of Taiwan Public TV since 2016 to 2022.

Dr. Wei-Ping Li is a postdoctoral researcher at the Philip Merrill College of Journalism at the University of Maryland and a research fellow at the Taiwan FactCheck Center, where she monitors and analyzes false information disseminated in the Chinese-language world. Her research focuses on the transnational dissemination of disinformation, propaganda, and media policy. Dr. Li received her PhD degree from the University of Maryland and an LL. M. degree from the University of Pennsylvania. Before pursuing an academic career, she offered consulting services on digital human rights and was a journalist based in Taiwan.

Introduction

Niklas Swanström and Filip Borges Månsson

The spread of disinformation has been a longstanding issue since the establishment of communication between societies. It has been used as a tool to spread propaganda and deceive adversaries in the political and intelligence sphere for centuries. In modern times, the internet has provided extensive opportunities to spread misinformation and manipulate information on a global scale. Western liberal democratic states, due to their open societies, have been heavily targeted by adversaries aiming to cause political turmoil, distrust, and instability through the effective use of disinformation and manipulation of information campaigns.

The digital age has ushered in an era where the manipulation of information has become a potent, and easily accessible, tool in the arsenal of statecraft. Potential adversaries like Russia and the People's Republic of China (PRC) have used disinformation to further their strategic goals, create discord, influence elections in democracies, and shape global narratives. While the focus is often on the individual disinformation efforts of these nations, understanding their potential collaboration in this area reveals the depth and complexity of the challenge faced by liberal democracies.

Russia has been utilizing aggressive and multifaceted disinformation tactics, particularly in Europe, to exploit existing divisions and undermine trust in democratic institutions. This includes strategic disinformation campaigns, cyber operations targeting foreign elections, and the weaponization of media through state-controlled outlets like RT (formerly Russia Today) and Sputnik News. These efforts aim to destabilize Western democracies and amplify societal divisions. Since the Russian invasions of Georgia in 2008, the annexation of Crimea in 2014, and the full-scale invasion of Ukraine in February 2022,

there has been an unprecedented disinformation campaign, with Ukraine as a primary target. This has led EU member-states to urgently ramp up policies and measures to counter disinformation.[1] Furthermore, Russia's cyber operations, including hacking, leaking sensitive information, and social media manipulation campaigns, have been deployed to influence political processes and undermine adversaries' credibility. Russia has demonstrated its ability to wield information as a weapon of mass disruption by exploiting vulnerabilities in digital ecosystems.

In parallel, the PRC seems to have adopted a more calculated approach to disinformation, primarily aimed at bolstering its international image and advancing its geopolitical interests. On an internal level, the PRC's information manipulation strategy has been embedded in its promotion of digital authoritarianism, focusing on utilization of propaganda and censorship measures through robust internet surveillance within the Great Firewall, and in turn exerting tight control over information flows within its borders, shaping public opinion and quashing dissent.

Meanwhile, through a vast propaganda machinery comprising state-controlled media outlets like Xinhua News Agency and China Central Television (CCTV), Beijing seeks to shape global narratives in its favor while stifling dissent and criticism of its policies. The PRC's disinformation strategy extends beyond traditional media channels to include social media manipulation and information control. The Chinese Communist Party (CCP) leverages both overt and covert methods to influence discussions on platforms like Twitter and Facebook, deploying state-sponsored trolls and bots to amplify pro-China narratives and silence dissenting voices often through the United Front Work Department, the Chinese Communist Youth League (CYL), the Ministry of State Security (MSS), and Taiwan Affairs Office. Themes of Chinese disinformation often revolve around promoting the superiority of PRC's political system and economic

1 "The fight against pro-Kremlin Disinformation." Consilium, January 20, 2023, https://www.consilium.europa.eu/en/documents-publications/library/library-blog/posts/the-fight-against-pro-kremlin-disinformation/.

achievements while undermining Western democracies and portraying them as morally corrupt. Recent disinformation campaigns orchestrated by the PRC demonstrate an expanding array of tactics, addressing a range of topics such as AUKUS, Russia's war in Ukraine, and COVID-19, thus extending beyond issues related to domestic or territorial governance.[2]

PRC's ambitions in Taiwan and the South China Sea highlight the extent of PRC's disinformation campaigns. More notably Taiwan, given its tense and complicated relationship with the PRC, has been at the forefront of Chinese disinformation campaigns, constantly exposed to the PRC's propaganda first hand before its techniques are deployed on a global scale. Portrayed as a 'testing ground,' Taiwan has served as a critical 'gateway,' disseminating disinformation to other regions.[3]

The PRC's expansion of disinformation is supported by advancements in AI and quantum technology, making it more effective than Russia's older technology, even though Russia has long been a master of traditional disinformation and has to some extent set the standard for the PRC. It is important to consider how innovative technologies have changed and improved strategies for both the PRC and Russia.

There is a growing consensus among a broad spectrum of countries about the imperative to counter the PRC's coercive behavior in the information space. Many nations express mounting apprehension regarding PRC's continued propagation of pro-Kremlin propaganda and disinformation regarding Russia's conflict with Ukraine. EU member-states are not exempt from the disinformation campaigns orchestrated by the PRC. According to the annual

2 U.S. Department of State, "How the People's Republic of China Seeks to Reshape the Global Information Environment," September 28, 2023, Global Engagement Center Special Report, 38, https://www.state.gov/wp-content/uploads/2023/10/HOW-THE-PEOPLES-REPUBLIC-OF-CHINA-SEEKS-TO-RESHAPE-THE-GLOBAL-INFORMATION-ENVIRONMENT_508.pdf.

3 Shih-Shiuan Kao, "Taiwan's Response to Disinformation a Model for Coordination to Counter a Complicated Threat," National Bureau of Asian Research (NBR). September 2021, https://www.nbr.org/wp-content/uploads/pdfs/publications/sr93_taiwan_sep2021.pdf.

report from the Swedish Military Intelligence and Security Service (MUST), as the PRC holds strategic interests related to the Arctic and Space industry, Sweden has continuously been exposed to attempts to influence Swedish public opinion and discourse, whilst conducting unauthorized surveillance and intelligence activities.[4] Additionally, several European states have been under heavy pressure from the PRC, such as Lithuania, Sweden, and Norway to mention a few.

While Russia and the PRC pursue distinct, sometimes very different, objectives through their disinformation efforts, there are indications of potential collaboration in certain spheres. Both nations share an interest in challenging Western hegemony, undermining democratic institutions, and advancing their respective geopolitical agendas. The prospects of deepening ties and collaborations have been further strengthened since the war in Ukraine, with PRC and Russia's announcement of a "no-limits partnership" in 2022 aimed at strengthening the bonds and dialogues President Putin and Xi (albeit with the PRC positioning itself cautiously regarding Russia's invasion of Ukraine). However, on March 7, 2024, member of the Political Bureau of the CPC Central Committee and Foreign Minister Wang Yi further reiterated on the PRC-Russia relations by stating that their "strategic partnership of coordination has been moving forward on a higher level", highlighting that their cooperation remains mutually beneficial and that they continually seek to deepen their "strategic coordination". This, in Yi's view, is believed to be a strategic choice by both parties.[5] Yet, how mutual the partnership is remains to be seen as the no-limits partnership has previously suggested a discrepancy in the newly presented narrative, as Russia has been more dependent on the PRC rather than the contrary.[6] Bearing this into consideration, this convergence of interests

4 Must årsöversikt 2023, (n.d.), https://www.forsvarsmakten.se/siteassets/2-om-forsvarsmakten/dokument/musts-arsoversikter/must-arsoversikt-2023.pdf.

5 "Wang Yi: China and Russia have forged a new paradigm of major-country relations that differs entirely from the obsolete Cold War approach 中华人民共和国外交部," (n.d.). https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/202403/t20240308_11256414.html.

6 Amy Hawkins, "Year of War in Ukraine tests China's "no limits" relationship with Russia," The Guardian, February 24, 2023, https://www.theguardian.com/world/2023/feb/24/ukraine-war-china-russia-no-limits-relationship.

raises questions about the extent of collaboration between Russia and the PRC in the realm of disinformation and its implications for global stability. As liberal democracies grapple with the growing threat of disinformation, it is essential to recognize the interconnected nature of these challenges. By understanding the strategic goals, tactics, and potential collaboration between Russia and the PRC, policymakers can develop more effective strategies to counter the spread of misinformation and safeguard democratic principles in the digital age.

As the introductory remarks highlight, it is imperative to understand the implications of disinformation as a tool in the digital age, and how authoritarian states like the PRC and Russia systematically use it to their advantage. Albeit in different manners, by understanding how the two states operate and use disinformation for their benefit, one can begin to draw patterns to see of the two states may (or may not) collaborate on that front, whilst also provide some needed insights on how western democratic states, whom are heavily affected by disinformation and manipulation of information, may effectively counter disinformation whilst continuously valuing democratic values in a digital age that has in many aspects grown more polarized. This volume aims to outline the experiences in Asia and in Europe seeking to understand the commonalities and differences between the modus operandi used by Moscow and Beijing. It also explores whether these states cooperate formally or informally. Additionally, it includes forward-looking chapters that discuss how democratic societies can and should collaborate to address the modern challenge of disinformation.

1. Cognitive Warfare and Disinformation by Authoritarian States: A Case Study in Taiwan

Wen Cheng Fu and Wen Jian Huang

Since 2014, Russia has conducted cognitive warfare strategies in Crimea, combining disinformation on social media with military drills to significantly influence public opinion and national identity. This led to over 97 percent of Crimea's population supporting annexation by Russia, seen as a cognitive victory achieved at minimal military cost. Since then, the authoritarian state's cognitive warfare on social media has become a new form of conflict that is drawing global attention. By February 2022, after a series of cognitive tactics by Russia, the situation escalated into a physical war with Ukraine.[1] The Atlantic Council noted that with the rapid development of digital and social media, warfare has changed, particularly in the human and cognitive domain, where disrupting existing social networks and exacerbating domestic divisions have become key strategies to influence battlefield outcomes. Disinformation has emerged as a new form of warfare.[2]

The strategies of cognitive warfare through disinformation exploit certain weaknesses in democratic regimes because public opinion is easily disseminated by media. Most democratic countries consider freedom of speech, internet freedom, and freedom of action as fundamental human rights, making it

1 Georgii Pocheptsov, "Cognitive attacks in Russian hybrid warfare," Information & Security, September 2018, https://isij.eu/system/files/download-count/2023-01/4103_pocheptsov_cognitive_attacks.pdf.

2 Digital Forensic Research Lab, "Undermining Ukraine: How Russia widened its global information war in 2023," Atlantic Council, February 29, 2024, https://www.atlanticcouncil.org/in-depth-research-reports/report/undermining-ukraine-how-russia-widened-its-global-information-war-in-2023/.

difficult for governments to verify information. Cognitive warfare achieves low-cost, high-impact influence through a series of mutually reinforcing disinformation mechanisms. This includes highly specious but hard-to-verify disinformation on social media, linking multiple layers such as schools, religious institutions, online influencers, and international media, forming robust disinformation networks. China's cognitive warfare against Taiwan has been escalating, involving various aspects like legal warfare, public opinion warfare, psychological warfare, and united front tactics. The goal is to undermine government authority, divide national identity, and polarize societal emotions.[3]

Regarding the channels of disinformation dissemination, Chinese PR firms like Shanghai Haixun Technology have utilized over 70 fake news websites to spread information aligned with Chinese state interests worldwide. These include sites disguised as independent news outlets, such as "Fortune Taiwan" and "Taiwan Focus," distributed across various social media platforms. The application of information technology has made social networking sites and instant messaging apps the main sources of daily information and social activity. The anonymity and speed of the internet enable tactical behaviors to expand effectively; carefully designed propaganda campaigns targeted at specific community groups can more effectively achieve the goals of incitement and division, rivaling the influence of traditional weaponry.[4]

Analysis of disinformation attacks by China and Russia reveals two key steps. First, they use psychometrics to understand target audiences, such as hacking meeting records and emails to gather information, identifying target groups, and analyzing and categorizing large datasets. Second, they build models and algorithms based on these analyses to test how specific narratives and stories trigger emotional and political responses from different groups.

---

3 Nathan Beauchamp-Mustafaga, "Cognitive Domain Operations: The PLA's New Holistic Concept for Influence Operations," *China Brief*, May 14, 2021, https://www.rand.org/pubs/external_publications/EP68632.html.

4 "Seize control over future wars and safeguard national cognitive space security," 解放军报, June 16, 2014.

China's Cognitive Warfare and the Gray Zone of Disinformation

Recently, China has shifted away from crude tactics like launching cyberattacks on Taiwanese government websites, instead quickly grasping Taiwan's social dynamics, from setting agendas to guiding narratives.[5] It integrates the influence of mainstream and social media to create an atmosphere where fake news seems real. This nuanced approach to cognitive and psychological warfare, which combines both depth and breadth, has caused significant harm to Taiwanese society, necessitating a response model that aligns with Taiwan's national conditions and social realities.

According to the 2023 V-Dem (Varieties of Democracy) report by the University of Gothenburg, Taiwan has been the most frequently targeted country for foreign disinformation attacks for 13 consecutive years.[6] When U.S. House Speaker Nancy Pelosi visited Taiwan in 2022, Chinese state media released false news about PLA Su-35 fighter jets crossing the Taiwan Strait just before her plane landed.

However, many traditional media outlets lack the capacity and time for verification, often following Chinese state media reports or using PLA propaganda videos, inadvertently aiding China's cognitive warfare. Additionally, the BBC revealed that China uses the China Global Television Network (CGTN) to establish "influencer" departments that cooperate with foreign influencers to spread false and controversial information locally.[7] This tactic is also applied to Taiwan, using innovation bases to train young Taiwanese live streamers and collaborating with Taiwanese influencers. By leveraging social media habits in Taiwan, they embed Chinese propaganda messages or viewpoints in Facebook

5 James Andrew Lewis, "Cognitive Effect and State Conflict in Cyberspace," Center for Strategic and International Studies, September 26, 2018, https://www.csis.org/analysis/cognitive-effect-and-state-conflict-cyberspace/.

6 T. K. Gastaldi, "Defiance in the Face of Autocratization," Varieties of Democracy (V-Dem), March 2023, https://www.v-dem.net/documents/29/V-dem_democracyreport2023_lowres.pdf.

7 C. L. Hung, W. C. Fu, C. C. Liu, and H.J. Tsai, "AI Disinformation Attacks and Taiwan's Responses during the 2024 Presidential Election," Taiwan Communication Association, April 12, 2024, https://www.thomsonfoundation.org/media/268943/ai_disinformation_attacks_taiwan.pdf.

live broadcasts, adopting a "Taiwan pulling Taiwan" strategy to persuade and draw in Taiwanese people. Before Pelosi's visit, influencers on Facebook started live broadcasts, calling Pelosi's visit a disaster that would turn Taiwan into cannon fodder, even resorting to personal curses against her, with hashtags like "#NationalUnificationIsImperative" (#祖國統一是必然) appearing in posts.

In recent years, many instances of China's military manipulation against Taiwan involve unverified images, such as Chinese military aircraft near Penghu entering Taiwan's ADIZ, or PLA troop build-ups along the coast, causing anxiety among Taiwanese citizens. Many media outlets, without verification, mention only "unofficial confirmation," yet extensively report and spread these images. This creates opportunities for cognitive warfare, using disinformation and contentious information to intensify already divided social communication environments, causing supporters of different positions to close the door to communication, further deepening gaps and hostilities, and having a profound impact on national security.

Another mode involves leveraging significant government decisions to quickly guide issues and influence public opinion. For example, when China announced 31 policies towards Taiwan, fake news reports immediately appeared online, claiming hundreds of university professors had gone to work in China. Another approach is entirely initiated by China; for instance, last year, the PLA Air Force posted a photo of an H-6K flight on Weibo, with discussions suggesting the background mountains were Taiwan's Mt. Jade. Although the Taiwan Ministry of National Defense later clarified that this news was fake and so was the background, this unverified news had already sparked heated and widespread discussions on domestic BBS and social media platforms like Facebook, Line, and WhatsApp. This has affected the military's image and diminished public confidence in national defense policies and military preparedness.

The Disinformation Industry Chain and Its Impact

Recently, Twitter, a major social media platform with over 330 million users worldwide, announced it had identified over 230,000 accounts suspected of spreading disinformation during the COVID-19 pandemic. Of these, 170,000

accounts were clearly linked to the Chinese government and had violated Twitter's manipulation policy, impacting international stability. Twitter has permanently removed these accounts.[8]

The Atlantic Council's Digital Forensic Research Lab pointed out several key indicators of China's cognitive warfare efforts during the COVID-19 pandemic.[9] Firstly, many propaganda accounts, such as "Free Northeast Radio", were recently registered, never posted original content, and retweeted only positive news about China's pandemic response, such as providing essential medical supplies to Italy and Spain. Secondly, these accounts uniformly promoted conspiracy theories. These accounts created a false mainstream opinion on the internet, influencing global perceptions of China's pandemic response, and providing evidence of cognitive warfare combined with external propaganda. Unaware of these tactics, many people are easily swayed by such disinformation.

To thoroughly expose China's manipulation of cognitive warfare, Twitter submitted the user data of abnormal behaviors during the COVID-19 pandemic to institutions like the Australian Strategic Policy Institute and the Stanford Internet Observatory for verification. Both institutions confirmed that more than 23,000 manipulated fake accounts were created in late 2019, mostly posted in local languages but accompanied by images with Chinese text. In addition, the researchers found that these unusual accounts often posted tweets regularly between 8 a.m. and 5 p.m. BST, with significantly fewer tweets on weekends. This regular posting frequency differs from the usual "normal" user's use of social networking sites after work and on weekends, demonstrating inauthentic behavior in these accounts.

8 Puma Shen, "The Chinese Cognitive Warfare Model: The 2020 Taiwan Election," Prospect Quarterly, January 2021: 1-66, https://www.pf.org.tw/wSite/public/Attachment/003/f1646210580296.pdf.

9 AFP, "Diplomatie chinoise: Pékin sauveur ou loup combatant [Chinese Diplomacy: Beijing, Savior or Fighting Wolf]," May 26, 2020, https://www.lepoint.fr/monde/diplomatie-chinoise-pekin-sauveur-ou-loup-combattant-26-05-2020-2376999_24.php (accessed January 16, 2024).

A detailed examination of China's cognitive warfare institutions revealed that the Chinese Ministry of Foreign Affairs, the Propaganda Department, and the United Front Work Department are the primary sources of cognitive warfare, coordinated with state and civilian media outlets like the People's Daily, Xinhua News Agency, CCTV, Global Times and Tencent News as the main channels of cognitive warfare.[10] Its impact includes various self-media pages on Facebook in different countries and poorly verified international media like Asahi Shimbun and World Journal. After forming a false "international public opinion," local opinion leaders and fan pages follow, forming a sophisticated disinformation industry chain.[11]

TikTok presents two main national security risks as its global popularity grows. First, concerns about personal privacy and data protection have arisen, with countries like the U.S. and the UK accusing TikTok of collecting and sharing users' personal information and behavioral data, threatening privacy and data security. The company can gather and store sensitive data such as location, contacts, and browsing history, which could be used for targeted advertising or sold to third parties. In addition, China's National Security Law mandates that the government has the authority to request all data collected by companies, potentially leading to misuse or sharing of user data.[12]

Second, with a global user base, TikTok can be utilized to spread fake news and misinformation, influencing elections and political situations in other countries. While TikTok appears to be a social platform for sharing short videos, it also hosts issues related to hate speech and disinformation. The U.S.

---

10 Wenna Zeng and Coin Sparks, "Popular nationalism: Global times and the US–China trade war," International Communication Gazette, October 2019: 26-41, https://journals.sagepub.com/doi/10.1177/1748048519880723.

11 Zhao Alexandre Huang and Rui Wang, "Exploring China's Digitalization of Public Diplomacy on Weibo and Twitter: A Case Study of the U.S.-China Trade War," International Journal of Communication, 2021: 1912-1939, https://ijoc.org/index.php/ijoc/article/download/15105/3422?__cf_chl_tk=VGc68fVzHTW9gdy3QsOPtWbFIhOXSUQCL3zEr_GSNG8-1724942465-0.0.1.1-4820.

12 Nathan Beauchamp-Mustafaga, "Cognitive Domain Operations: The PLA's New Holistic Concept for Influence Operations," China Brief, May 14, 2021, https://www.rand.org/pubs/external_publications/EP68632.html.

government found that some users posted content with racism, sexism, or other hate speech, potentially harming others and causing social division.

Strengthening and Weakening Democratic Resilience

Disinformation and cognitive warfare have infiltrated societies, becoming a non-traditional security issue impacting social stability and national security. Combating disinformation requires diverse approaches across technology, law, journalism, social psychology, and education. Among prevention measures such as platform self-regulation, legislative action, establishing fact-checking agencies, media self-discipline, and media literacy education, legislative action urging platform operators to take social responsibility has been most effective. Future efforts depend on cooperation among governments, media, and platforms to create a cleaner online space, allowing Taiwanese society to pursue development and progress in stability.

"Intellectual self-defense" is crucial for preventing disinformation and cognitive warfare. This involves training in critical thinking and logical argumentation to evaluate messages and identify fallacies and misinformation in digital information. Besides identifying fake news, establishing "digital hygiene" practices, such as verifying information before sharing, is essential.

As social media increasingly plays a vital role in national and defense security, data privacy and information security issues gain more attention. With emerging technologies like AI and IoT, the demand for personal data protection continues to rise. Governments can enact stricter laws and regulations to protect user data and privacy. Although Taiwan has established laws such as the Personal Data Protection Act and the Communication Security and Surveillance Act, further regulation of foreign media platforms is necessary. This would require tech companies to protect user data and privacy adequately, preventing specific state powers from manipulating and controlling the media.

Another reason democracies can only respond passively to disinformation is that, before the Cambridge Analytica scandal, social media positioned itself as a "communication platform," with all content generated by users, making

users responsible for media content. However, after the scandal, it became clear that user data collected by social media could provide scientific evidence for cognitive warfare targets.

In summary, with advancements in mobile communication technology and the widespread use of social media and messaging apps, false information with political or commercial objectives spreads widely on the internet, confusing the public and interfering in the internal affairs of other countries, affecting election results, and posing threats to social stability, national security, and democratic development. Therefore, disinformation is a concern for many countries, leading to various countermeasures to combat false information.

Additionally, combining domestic and international research institutions to analyze the social network and cognitive warfare message dissemination behavior of specific platforms frequently attacked can help quickly respond to large-scale online attacks.

Integrating domestic media, public media, and fact-checking organizations to observe and track disinformation and cognitive warfare content over the long term can effectively prevent the spread of cognitive warfare and its impact on society, while upholding freedom of expression in democratic countries.

In conclusion, understanding single-point online attack behaviors, collaborating with think tanks for coordinated responses, and integrating third-party fact-checking agencies marks a shift from single-point blocking to diversified responses. This aims to develop a "Taiwan model" to counter the growing psychological and cognitive warfare attacks on Taiwan's social stability.

2. The Case of Estonia: Navigating Disinformation in the Shadow of Russian Influence

Marek Kohv

By illustrating how Russia has been using disinformation against Estonia ever since it regained independence, this chapter proves that although the Kremlin's propaganda machine is extremely powerful, in the grand scheme of things, it is also one-wheeled.

Russia does not (and cannot) create unique problems in foreign societies; it only takes advantage of the existing ones. Therefore, a well-validated axiom states that to combat this type of information influence, a country must find the root of a society's problem and tackle it.

The effectiveness of Russian and, indeed, any propaganda is attributed to the so-called 'firehose of falsehood.'[1] Under this model, Moscow broadcasts similar narratives against Estonia to both Estonian and international audiences to create the most favorable conditions to advance its own foreign policy goals.

A Lesson in History

To understand the main Russian narratives employed towards and against Estonia, one must first understand the historical context. Estonia has been a target of Russian influence operations for decades. One might even argue that systematic anti-Estonian campaigns started as soon as the nation won its independence in 1918. The most blatant manifestation of that period was the

1 Christopher Paul and Miriam Matthews, "The Russian "Firehose of Falsehood" Propaganda Model," Rand Corporation, 2016: 4, https://www.rand.org/pubs/perspectives/PE198.html.

attempted coup by the Soviet Union in 1924. Yet, the Estonian state managed to withstand this hybrid aggression from the Soviet Union until it was occupied by the Red Army in 1940.

In parallel with committing atrocious crimes within the occupied country's borders, the Kremlin was conducting an information campaign against the Estonian people internationally. It was systemically trying to convince the foreign public that Estonia's accession to the Soviet Union was not only a voluntary decision but also an objective course of history.

To this end, history books were written and rewritten, while witnesses and dissidents were either executed or deported and replaced with ideological supporters of and from the Soviet Union, thereby creating a large Russian-speaking minority in the country. By the end of the Soviet era, the number of people of other nationalities in Estonia had increased to about 600,000 and constituted 38 percent of the republic's population.[2] They would soon be used as the main asset of Russian propaganda against independent Estonia.

Estonia, nonetheless, managed to preserve the memory of statehood and independence and regained both in 1991. One of the first and most important challenges for the country was the expulsion of Russian troops from its sovereign territory. The supposed violation of minority rights became the main narrative accompanying that process. The allegation has proven to be such a persuasive message that it is alive and well in Russian propaganda to this day. It took Estonia several years of diplomatic efforts, and by August 31, 1994, it finally carried through the withdrawal of active personnel but had to concede that Russian military retirees would stay as a compromise.

The year before the departure of the Russian troops, the young Estonian state had to deal with an illegal referendum in the eastern border region Ida-Virumaa, which Moscow probably instigated. Ida-Virumaa was going through acute

2 Eesti Entsükolpeedia, "Rahvastiku ränne Eestis," http://entsyklopeedia.ee/artikkel/rahvastiku_r%C3%A4nne_eestis (accessed August 30, 2024).

socio-economic problems because several enterprises, previously reliant on the Soviet Union, were struggling. Moreover, the local population employed across the border in Russia received salaries in rubles, hence their spending capacity in Estonia was limited.

Russian speakers on both sides of the border were further upset about the passing of two laws—on foreigners and on local government elections—that regulated the rights of non-Estonian citizens. The Law on Foreigners stipulated visa, residence and work permit requirements as well as laid down the conditions for deportation of those staying in the country illegally. The Local Government Organization Act prescribed that only Estonian citizens could run for elected offices but allowed non-citizens to vote at the local level. Nonetheless, it meant that Russian citizens in Ida-Virumaa would lose their public administration jobs and the political power that came with them.

The pro-Russian authorities—led by then-Chairman of the Narva City Council Vladimir Chuikin who was a Russian citizen and, therefore, would no longer be able to keep his office—held an illegal referendum in an attempt to veto the new legislation. The referendum asked the residents of the cities of Narva and Sillamäe whether they wanted "to have the status of national-territorial autonomy within the Republic of Estonia." With the turnout at 53 percent, 97 percent voted in favor of the referendum. However, the Estonian Constitution only permits a nationwide referendum, so the Supreme Court predictably declared the local vote invalid.[3]

Aside from its illegality, why did the referendum fail to generate a higher turnout and public support? The government in Tallinn realized the gravity of the situation and comported itself accordingly. Indrek Tarandi, then special government representative to Narva, attributes the fiasco of the pro-Russian forces to the fact that there were no Russian troops present on the ground (they had not yet completely withdrawn at that time but were stationed further in

3 Kaspar Koort, "Ajaloolugu: kuidas Ida-Virumaa Eestile jäi," Postimees.ee, October 26, 2017, https://tartu.postimees.ee/4288807/ajaloolugu-kuidas-ida-virumaa-eestile-jai.

the west of the country). Moscow could not help either: in 1993, it saw a bitter domestic power struggle of its own. By contrast, the Estonian government had strong international support, especially from Swedish Prime Minister Carl Bildt.[4]

The Kremlin did use disinformation and threatening rhetoric against Estonia but primarily for internal political reasons or to negotiate better conditions for its military retirees. Nonetheless, that campaign cannot be dismissed as ineffective. Estonia's Russian-speaking community still lived in the Russian information space and thus consumed false information on a daily basis. The local pro-Russian forces and backers of the referendum repeated the same narratives after the senior Kremlin officials. A Narva newspaper, for example, claimed that a genocide of Russians was underway in Estonia.[5]

One can only comprehend the real danger of such a referendum when taken in the historical context: at the same time, Russia successfully contributed to the territorial conflict in Moldova's Transnistria, which has not been resolved to this day.

The Return of Russia

One might argue that Moscow had less attention and fewer resources to spare on disinformation campaigns in the 1990s, as Russia itself was suffering from domestic political and social turbulence. An absurd example of such early demonization was the legend about the "Baltic female snipers in white tights," who allegedly fought against the Russian forces in Chechnya and even the Georgia-Abkhazia war.[6]

---

4 Maarja Pakats, "Referendum, mis kukkus läbi. Kuidas Narva üritas Eesti vabariigist lahti rebida," Delfi.ee, August 4, 2021, https://www.delfi.ee/artikkel/94199353/referendum-mis-kukkus-labi-kuidas-narva-uritas-eesti-vabariigist-lahti-rebida.

5 Ivan Lavrentjev, "Ivan Lavrentjevi vastulause Mihkel Mutile: jutt Narva autonoomiast kätkeb endas ohte," Postimees.ee, June 29, 2017, https://arvamus.postimees.ee/4161803/ivan-lavrentjevi-vastulause-mihkel-mutile-jutt-narva-autonoomiast-katkeb-endas-ohte.

6 Aivar Jürgenson, "Balti naissnaiprid Gruusia-Abhaasia ja Tšetšeenia sõdades: Vene sõdurilegendi funktsioonid ja ajaloolised juured," *Ajalooline Ajakiri* 182, no. 4 (2022): 261, https://ojs.utlib.ee/index.php/EAA/issue/view/1869

Yet, when Vladimir Putin came to power, many old Russian doctrines were revived and an enforcement directive on the new foreign policy directive was signed. The latter set three priorities for Russia's foreign service: strengthening its national security, fostering favorable conditions for trade and economic growth, and protecting the rights of the Russian-speaking minority in the Commonwealth of Independent States (CIS) and Baltic states. The doctrine of informational security, which dealt more precisely with influence activities, came into force. All those doctrines expressed one goal—i.e., to restore Russia's influence, at least on the territory of the former USSR. Russian information channels tried to craft propaganda narratives aimed at the 'near abroad' and aggrandize "the aspirations and longings of the Russian people" in the neighboring countries, which should be heeded. At the same time, the narrative about the 'artificial nature of the post-Soviet states' was pushed.[7]

In the context of this suggestive propaganda, it did not matter which channels would be used or how; the only goal was to achieve a result that would be favorable to the Kremlin. For instance, in an attempt to prevent Estonia from joining the EU and NATO, the country was being portrayed as an unreliable international partner. For this, traditional media were employed, yet their reports were full of fact-twisting or outright lies, with the most popular storyline being the one about the persecution of the Russian-speaking minority.

Although the Baltic countries laid most of the groundwork for the eventual membership in the 1990s, the historic window of opportunity opened only after the 9/11 attack when NATO and Russia went on a joint crusade against terrorism.[8] The attitude of indifference towards Estonia was somewhat illustrated by Putin's comment: "I think it would be a tactical and strategic mistake to prevent Estonia from joining NATO. If Estonia wants to join, let

7 Juhan Värk, "Venemaa positiivse hõlvamise poliitika ja teiste välispoliitiliste liinide mõjud Eesti-Vene suhetele aastail 1991-2011," Tallinna Tehnikaülikool, 2012: 134, https://books.google.ee/books/about/Venemaa_positiivse_h%C3%B5lvamise_poliitika.html?id=2goOrgEACAAJ&redir_esc=y.

8 Kadri Liik and Argo Ideon, "Eesti tormiline teekond: Moskva vangikongist NATO kaitsva vihmavarju alla," Postimees.ee, November 19, 2002, https://www.postimees.ee/1980605/eesti-tormiline-teekond-moskva-vangikongist-nato-kaitsva-vihmavarju-alla.

it join if it thinks it is best for it. I don't see any tragedy in that."[9] Estonia's accession to NATO and the EU significantly diminished Russia's ability to tarnish its international image—with a seat at the table, Estonia could immediately respond and refute any false information.

Russia's Modus Operandi

With such a rich history of defending against—as well as combatting—Russian influence operations, Estonia has developed a workable toolkit. *Propastop*, a volunteer-run Estonian blog that specializes in monitoring and debunking Russian propaganda, adopted several criteria that help to identify a vehicle of the Kremlin disinformation. Those include 1) a connection between the owner (operator) of a media channel and the Russian establishment; 2) precedents of the (re-)broadcasting of Kremlin propaganda; and 3) sanctions already imposed against it in other countries. Below is the list of known malign actors in Estonia.[10]

- **Pervõi** (*Первый канал*) and its offspring **Pervõi Baltiiski Kanal** (*Первый Балтийский канал,* PBK) are best known for their *Вре́мя* daily news program. PBK formally belongs to the Baltic Media Alliance (BMA) and produces its own content but also transmits that of the Russian state media, which comes with the Kremlin perspective and biases.

- **Rossija, Rossija 1, Rossija 24, RTR Planeta,** and **RTR Planeta Baltic** are 100 percent owned by the Russian government and do not hide their pro-government views. Their programs often feature Estonia-related speakers who criticize the country.[11]

- **REN TV, Ren TV Baltic,** and **REN TV Eesti** belong to the BMA, rebroadcast many of the Pervõi's content, and have even recruited Anna Chapman, an infamous Russian intelligence agent, as a TV host.

---

9 Marko Mihkelson, "Venemaa: Valguses ja Varjus," Varrak, 2010, 245.

10 Propastop, "Propagandakanalite välimääraja: osa 1," April 24, 2016, https://www.propastop.org/2016/04/28/propagandakanalite-valimaaraja-osa-1/.

11 Estonian Internal Security Service's Yearbook 2015, https://kapo.ee/sites/default/files/content_page_attachments/Annual%20Review%202015.pdf.

- **NTV, NTV Mir,** and **NTV Mir Eesti**, once independent, are now owned by Gazprom Media (and through the BMA in the Baltic states) and employed by the government attack the Russian opposition.
- **RT** (formerly **Russia Today**) and the **Sputnik** multimedia portal are the main vehicles of Russian propaganda abroad.
- **Zvezda** is a TV channel owned by the Russian defense ministry that articulates the Kremlin's positions regarding developments in neighboring countries.

Aside from the media, the Kremlin maintained a wider network of its agents of influence. In the 2000s, the Union of Russian Compatriots Associations in Estonia (with its affiliates) and the Human Rights Information Centre (operating under the direction of the Russian embassy in Tallinn) acted as Russia's main lobbyists while financially dependent on Russia. The Estonian Internal Security Service recalls that they used to plant the narratives accusing the Baltic states of 'fascism' (a more prominent buzzword for Russian speakers than Nazism). This technique was devised to galvanize foreign political pressure, primarily through the Jewish community.[12] Today, Russia employs the same rhetoric with the same purpose against Ukraine.

To help navigate this vast and complex ecosystem, *Propastop* has categorized the networks of 'Russian compatriots' that used to be active in Estonia:

- The **Protestors** (Protestijad) organized and participated in protests.
- The **Guard** (Valveaktivistid) is the largest network of activists who 'represented' Estonia in international organizations but, in essence, abused such platforms to accuse the Estonian state of human rights violations and discrimination against the Russian-speaking minority.[13]

12 Estonian Internal Security Service yearbook 2004, https://kapo.ee/sites/default/files/content_page_attachments/Annual%20Review%202004.pdf.

13 Propastop, "Russia-related networks in Estonia Part 1," May 29, 2018, https://www.propastop.org/eng/2018/05/29/russia-related-networks-in-estonia-part-1/.

- The **Propaganda media handlers** (Propagandameedia käsilased) manage the propaganda portals *Baltnews* and *Baltija.eu* that mass-produced disinformation daily.[14]
- The **Propaganda Clubs** (Propagandaklubid) are connected to *Komsomolskaja Pravda*, a Russian newspaper, and the *Impressum* NGO that organized thematic discussions in Tallinn and invited speakers from Russia, whose talking points directly overlapped with those of the Kremlin and are predominantly anti-Estonian.[15]
- The **Nazi theme instigators** (Natsiteema õhutajad) were affiliated with the Russian *World without Nazism* movement financed directly by the Kremlin. The group was behind the Bronze Soldier Night riots in 2007.[16]
- The **Russki Mir** foundation**,** created in 2007 by Putin's order, operated in Estonia since 2008 and financed several local 'compatriot' projects. Some former Soviet Special Service officers and several extremist politicians were reportedly engaged.[17]

Moscow's Holy Crusade

Many memorials to the criminal Soviet regime have been taken down or removed across Europe since the collapse of the USSR, and Russia has not kept quiet about it. At times, Moscow even tried to interfere, using multiple levers.

The removal of the Bronze Soldier monument in Tallinn in 2007 and the T-34 tank on display in Narva in 2022 were two of the most vivid examples. Both were used by Russia and its local henchmen for provocations and hate speech against Estonia. In both cases, the government decided to move the monuments to more suitable locations: a military cemetery and a war museum,

14 Propastop, "Russia-related networks in Estonia Part 2," June 5, 2018, https://www.propastop.org/eng/2018/06/05/russia-related-networks-in-estonia-part-2/.

15 Propastop, "Russia related networks in Estonia Part 3," June 15, 2018, https://www.propastop.org/eng/2018/06/15/russia-related-networks-in-estonia-part-3/.

16 The activities in 2005-11 were widely covered by the Estonian Internal Security Service's annual reviews.

17 Propastop, "Russia-related networks in Estonia Part 5," July 24, 2018, https://www.propastop.org/eng/2018/07/24/russia-related-networks-in-estonia-part-5/.

respectively. In the first instance, the Kremlin launched a large-scale influence operation, feeding false information to the local Russian-speaking minority in order to mobilize it for riots that eventually erupted in downtown Tallinn. The removal of the tank in August 2022, on the other hand, did not trigger any similar violence, which must have been, at least in part, connected to the full-scale Russian war already raging in Ukraine.

The desecration of Estonia's historical sites has become less common over time but still occurs, with the latest case in early 2024. The Internal Security Service arrested two men on suspicion of defacing the Sinimägede (Blue Hills) battlefield memorial in Ida-Viru County; they reportedly received orders from Russia.

Apart from weaponizing history and memory, the Kremlin heavily relies on the Russian church as a tool of its influence abroad. There are two Orthodox churches in Estonia: the Estonian Apostolic Orthodox Church (under the direct jurisdiction of the Ecumenical Patriarch of Constantinople) and the Estonian Orthodox Church of the Moscow Patriarchate. The Patriarch Kirill of Moscow has recently called for a holy war against the West which he accused of satanic influence, meaning the European values.[18] The Patriarch has also claimed that Ukraine must be a part of the 'Russian World' and that the entire 'post-Soviet space' (including Estonia) must remain within the sphere of influence of the Russian Federation, essentially implying that the Republic of Estonia should disappear.[19] The Estonian parliament (Riigikogu) designated the Moscow Patriarchate as an institution that supports Russia's military aggression and condemned the Patriarchate's actions for justifying and inciting the bloody war in Ukraine; 75 MPs (out of 101) voted in favor.[20]

18 Brian Mefford, "Russian Orthodox Church declares "Holy War" against Ukraine and West," Atlantic Council, April 9, 2024, https://www.atlanticcouncil.org/blogs/ukrainealert/russian-orthodox-church-declares-holy-war-against-ukraine-and-west/.

19 Serhii Shumylo, "The Russian World of Patriarch Kirill as an apology of anti-Christianity, xenophobia, and violence," Orthodox Times, April 23, 2024, https://orthodoxtimes.com/the-russian-world-of-patriarch-kirill-as-an-apology-of-anti-christianity-xenophobia-and-violence/.

20 Parliament of Estonia, "Riigikogu declared the Moscow Patriarchate an institution sponsoring Russia's military aggression," June 6, 2024, https://www.riigikogu.ee/en/news-from-committees/

The Estonian Constitution guarantees that everyone is 1) entitled to freedom of conscience, freedom of religion and freedom of thought; 2) freedom to belong to any church or any religious society; and 3) free to practice their religion unless this is detrimental to public order, public health or public morality.[21] Endorsing violent aggression while praying for the aggressor state, and its political and military leadership during church services clearly violates those principles.[22]

Founding Pillars of Estonia's Resilience

Drawing from Estonia's history, one can learn several important lessons as to how to resist influence operations by hostile actors beyond Russia and build resilience to malign disinformation.

First**, vigilance and straightforwardness**. The Estonian Internal Security Service began tracking Russian influence activities in the 1990s, with its findings reflected in annual reviews. By doing so, the government has established a tradition of transparency and communication with the public. Moreover, Estonia has plenty of professional journalists, as well as volunteer activists such as the Baltic Elves, who are skilled in investigating Russia's activities in the Baltic region. Publicity and exposure of their connection to the Kremlin are what Russian agents of influence fear the most.

Second**, societal cohesion**. The Estonian Security Policy (2023) prescribes that to maintain and increase cohesion in society, constant attention must be paid to manifestations that are meant to divide it—i.e., to minimize the impact by targeting the cause of the problem.

constitutional-committee/riigikogu-declared-the-moscow-patriarchate-an-institution-sponsoring-russias-military-aggression/.

21 The Constitution of the Republic of Estonia, https://www.riigiteataja.ee/en/eli/ee/521052015001/consolide.

22 Ministry of Interior, "Declaring the Moscow Patriarchate an institution supporting military aggression," Republic of Estonia, April 25, 2024, https://siseministeerium.ee/en/declaring-moscow-patriarchate-institution-supporting-military-aggression.

Third, **rapid response**. To prevent conflicts that might threaten the constitutional order, it is necessary to quickly identify information influence activities—including disinformation campaigns—and limit their spread. It must be done in parallel with raising awareness of constitutional values in society through strategic communication.[23] Hate-mongers must be shut down if necessary. Since the outbreak of the full-scale war in Ukraine, Estonia has restricted the Kremlin-controlled channels because they incited violence and justified crimes.

Fourth, **an allied front**. Estonia's response to disinformation builds on the European Union's approach.[24] To keep one's information space clean, it is essential to know the media ownership structure that often dictates their agenda. The EU's Audiovisual Media Services Directive (which Estonia adopted in 2022) provides for more effective means for intervention in the event of a threat.

Fifth, **high-quality alternatives**. The role of a free press cannot be overemphasized. Estonia ranks 6th on the World Press Freedom Index.[25] Separately, the Estonian state has invested in the development of local Russian-language media where the Russian minority can get objective information. As a result, the trust and popularity of the Kremlin-controlled media among the Russian-speaking community in Estonia has significantly decreased. This initiative, however, is firmly grounded in respect for press freedom; the Estonian state never interferes with editorial policies.

23 Parliament of Estonia, "Eesti julgeolekupoliitika alused 2023," https://www.riigiteataja.ee/aktilisa/3280/2202/3001/julgeolekupoliitika_2023.pdf (accessed August 29, 2024).

24 European Commission, "A multi-dimensional approach to disinformation," Directorate-General for Communications Networks, Content and Technology, 2018, https://op.europa.eu/en/publication-detail/-/publication/6ef4df8b-4cea-11e8-be1d-01aa75ed71a1/language-en (accessed August 27, 2024).

25 Reporters without Borders, "MAP - 2024 World Press Freedom Index," May 3, 2024, https://rsf.org/en/map-2024-world-press-freedom-index.

Sixth, **education** is considered to be the most effective tool in combating disinformation.[26] Since 2010, Estonian public schools have been teaching media literacy as part of their curriculum. High school students take a mandatory 'media and influence' course.[27] A master's degree program in Disinformation and Societal Resilience has been recently created at the University of Tartu to train strategic communication experts. Apart from the government, NGOs such as *Propastop* do a commendable job in raising public awareness of disinformation. Several media houses have created fact-checking sections.

Seventh, **the whole-of-government approach**. Estonia has created the Computer Emergency Response Team, whose job is to deal with digital security threats, and introduced online police officers, who monitor dis- and misinformation on the Internet to prevent it from translating into real-world crimes. The key institution is the Government Communication Bureau. It monitors both Estonian- and Russian-language media, traditional and social; leads interaction with media and online platforms, as well as political parties, through guidelines and briefings, including on foreign information influence; cooperates with the State Electoral Office and the Information System Authority and maps related interference risks, in particular to the electoral processes.

The effectiveness of Estonia's approach is evidenced by the fact that most of the actors and their networks exemplified in this chapter have already been shut down or expelled from the country. Yet, they are still relevant and important to study as the Kremlin tends to operate in different countries with the same pattern of activities.

26 Jon Bateman and Dean Jackson, "Countering Disinformation Effectively: An Evidence-Based Policy Guide," Carnegie Endowment for International Peace, January 31, 2024, https://carnegieendowment.org/research/2024/01/countering-disinformation-effectively-an-evidence-based-policy-guide?lang=en&center=global.

27 Amy Yee, "The country inoculating against disinformation," BBC, January 31, 2022, https://www.bbc.com/future/article/20220128-the-country-inoculating-against-disinformation.

3. Swedish Strategies to Combat Foreign Influence Operations

Johan Wiktorin

Introduction

During the NATO accession, Sweden was the target of an influence operation to slow down the process when Turkey objected to Swedish membership. By using the right to demonstrate and freedom of expression, an Iraqi man associated with Iranian militia in Iraq started to burn Qurans in Sweden.[1] These bootstrapped actions were hugely amplified by Western media which lost control of proportions as the man did not represent any movement, interest group or party. These deeds led to intense rhetoric in many Muslim countries and eventually to a storming of the Swedish embassy in Iraq by another militia.[2] Ankara had to tread carefully to balance its interests in the Middle East and in NATO. According to the Swedish Government, Russia was amplifying the disturbances to damage Sweden's interests and international reputation.[3]

This has not been the only case where Sweden has been subject to disinformation and influence operations. In the last decade, state actors such as Russia and China have strengthened their operations in this field to undermine the resolve of Sweden and influence Swedish decision-making to align with their own interests. The Chinese ambassador to Sweden 2017-2021, Gui Congyou

1 "Koranbrännaren kan kopplas till regimen i Iran," Dagens Nyheter, September 2, 2023, https://www.dn.se/sverige/koranbrannaren-kan-kopplas-till-regimen-i-iran/ (accessed August 24, 2024).

2 "Iraqi cleric Sadr flexes muscle with torching of Swedish embassy," Reuters, July 21, 2023, https://www.reuters.com/world/middle-east/iraqi-cleric-sadr-flexes-muscle-with-torching-swedish-embassy-2023-07-20/ (accessed August 11, 2024).

3 "Sweden says it's target of Russia-backed disinformation over NATO," Reuters, July 26, 2023, https://www.reuters.com/world/europe/sweden-says-its-target-russia-backed-disinformation-over-nato-koran-burnings-2023-07-26/ (accessed August 24, 2024).

applied 'wolf warrior diplomacy' to intimidate the Swedish press regarding its coverage of China. He also threatened the sitting government with trade sanctions due to actions Beijing did not like. He was summoned at least 40 times to the Swedish Foreign Ministry for his behavior, and eventually, he left his office.[4] Such campaigns are linked to the geopolitical objectives of these nations, which, in the long term, threaten Swedish national security.

In this current of turmoil where autocratic countries are challenging the rule-based order, the small state of Sweden is being affected by the struggle between the great powers. China and Russia are together advancing their interests by layering their partners in different tiers, to strike against what they see as an unfair world order.

Like the Cold War, the United States is in the crosshairs for these states and their allies. The Soviet Union saw the U.S.' global influence and the spread of capitalism and liberalism as a threat to communism and Soviet interests. The U.S. was perceived as the "main enemy"—the primary geopolitical and ideological adversary—which was used to mobilize the Soviet security services and justify the Soviet Union's own aggressive actions.[5]

China and Russia are not the only actors conducting influence operations. Iran, North Korea, and Cuba are also actively trying to destabilize, sway opinions and advance their interests and are openly collaborating to disrupt the "main enemy" and its relations with allies and partners.

For example, the Cuban government has attempted to influence the U.S. elections. Reports suggest it has tried to denigrate specific American candidates in Florida.[6] Cuba is also alleged to have agreed with China to let Beijing use

4 "SVT Nyheter erfar: Kinas ambassadör uppkallad till UD 40 gånger," *Sveriges Television*, January 20, 2020, https://www.svt.se/nyheter/inrikes/kinas-ambassador (accessed Spetember 3, 2024).

5 "Soviet Means for Intervening in Election Campaign and Vote in the United States During the Cold War," Warsaw Institute, June 4, 2021, https://warsawinstitute.org/soviet-means-intervening-election-campaign-vote-united-states-cold-war/ (accessed September 10, 2024).

6 "U.S. intelligence official says Cuban attempt to influence local races is underway," *Miami Herald*, August 11, 2024, https://www.miamiherald.com/news/politics-government/article290532664.html.

bases on its soil for SIGINT purposes.[7]

In a global sense we are, therefore, witnessing the rise of a *Five Lies-alliance*. It is obvious in the Russian war of aggression in Ukraine, where China, North Korea, and Iran actively support Russia with military equipment, industrial goods, and are parroting the Russian narrative regarding the war. Cuba is also participating in this endeavor. Russian state-controlled media are the main news providers about the war in Ukraine for Cuba's official press, whose news influences the Spanish-speaking population in North and South America.

All this creates a mosaic of messages and narratives, multi-channels to watch and analyze, thus making it harder for open democracies such as Sweden to detect and identify malicious influence until they have established some grip in the respective target group or achieved a hostile take-over or dependency of important infrastructure or technology. The battery company Northvolt recently found itself in a huge crisis after months of negative news regarding accidents and production problems stemming from its dependence upon Chinese equipment installed in its factories and which was operated by Chinese personnel.[8]

Sweden has earlier experience from the Cold War era when the nation organized itself to defend against a Soviet attack, which has been useful for crafting today's countermeasures. The current information environment demands, however, different solutions, as the mandate for psychological defense back then was more narrowly defined and more closely aligned with the Armed Forces.[9]

---

7 "Secret Signals - Decoding China's Intelligence Activities in Cuba, Center for Strategic & International Studies, July 1, 2024, https://features.csis.org/hiddenreach/china-cuba-spy-sigint/ (accessed September 30, 2024).

8 "Northvolt skulle skapa oberoende mot Kina – samarbetspartner hyllar diktaturen," *Dagens Nyheter*, September 4, 2024, https://www.dn.se/sverige/northvolt-skulle-skapa-oberoende-mot-kina-samarbetspartner-hyllar-diktaturen/ (accessed September 5, 2024).

9 "Totalförsvarets civila del - Framväxt och fall – erfarenheter för framtiden," MSB, 117-122, https://rib.msb.se/filer/pdf/30502.pdf (accessed July 30, 2024).

Swedish Strategies

The Swedish government itself has assumed a leadership role in advancing efforts against malicious manipulation at the national level. In the new National Security Strategy published in July 2024, no specific strategy to counter foreign influence operations has been formulated.[10] Instead, the government is trying to enhance systemic action by assigning specific responsibilities to different public agencies to implement incremental strategies in sectors of society. These strategies are so far piecemeal and involve different initiatives focused on identifying, countering and mitigating the impact of disinformation and can be seen as structured around six key pillars:

1. Agency Coordination

The close collaboration in and between the public sector, academia, and the private sector that was severed when the Warsaw Pact dissolved is being repaired. Recent administrations have worked hard to extend clear mandates and coordination among the agencies to increase the effect of countermeasures.

Established on January 1, 2022, the Psychological Defence Agency (MPF) plays a central role in Sweden's defense against foreign influence operations. Its mission is to detect, identify, analyze, and counter disinformation directed at Sweden from abroad. The agency has several restrictions in place for not influencing or to be perceived as influencing the internal political debate. Furthermore, it shall enhance societal resilience through education and produce detailed situational reports on foreign interference. The purpose could be to support decisions inside the government on current attacks or to improve understanding of the threat landscape for building capabilities.[11]

The Swedish Civil Contingencies Agency (MSB) was earlier a key player in the fight against disinformation, having previously trained nearly 6,000 civil

10 "Regeringens skrivelse 2023/24:163 Nationell säkerhetsstrategi," Swedish Government, July 4, 2024, https://www.regeringen.se/contentassets/125593e4516a49ce9b9ab942f49cca8d/232416300webb.pdf (accessed August 26, 2024).

11 Psychological Defence Agency, https://mpf.se/psychological-defence-agency (accessed September 10, 2024).

servants to manage disinformation. The department in MSB which was handling foreign influence operations was brought into MPF on its creation. MSB now instead focuses on coordinating communication regarding crisis preparedness, crisis management, and total defense.[12]

The collaboration displayed during the national election to the European Parliament 2024 serves as an example of how the agencies coordinate among themselves under a unifying purpose. Under the auspices of the Swedish Election Authority, a national election network where relevant agencies met regularly to collaborate on protecting the electoral process was a vehicle for coordination. The Agency for Psychological Defence (MPF) maintained special coverage of the European Parliament elections, conducted training initiatives, and offered parliamentary parties the opportunity for meetings to raise awareness related to improper information influence. The security authorities, i.e, the Swedish Defence Radio Establishment (FRA) and the Swedish Security Service (Säpo), fused their intelligence through the National Cyber Security Center (NCSC) to support the civil agencies.[13]

2. Education Including Media

Another important part of Sweden's strategy is to raise awareness through education. Swedish agencies have trained civil servants to recognize disinformation and improve critical thinking skills in the public. Teaching initiatives in schools and universities have integrated source evaluation and digital competence into the curriculum. Many education establishments also provide ongoing training for the teachers.

Swedish media and fact-checking organizations counter disinformation by fact-checking units and collaborating with international networks. This enhances

12 The Swedish Civil Contingencies Agency, https://www.msb.se/en/ (accessed September 10, 2024).

13 Swedish Parliament, "Svar på fråga 2023/24:942 Skydd mot påverkansoperationer i valet till Europaparlamentet [Protection against influence operations in the elections to the European Parliament]," Answer to written question 2023/24:942 by Prime Minister Carl-Oskar Bohlin, June 5, 2024, https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svar-pa-skriftlig-fraga/skydd-mot-paverkansoperationer-i-valet-till_hb12942/ (accessed August 1, 2024).

the quality of journalism and, thus, the public's access to verified information. In 2024, the Government merged two former agencies into one, the Swedish Agency for Media (SAM), which shall promote freedom of expression and raise the proficiency of the population regarding media and information at large. The educational system will also be an important channel for SAM to launch a project to deal with AI-driven disinformation intended to improve critical thinking and decrease antagonistic influence through AI.[14]

On every level there is progress to build knowledge. To illustrate the spread in society, Karlstad University has developed Master's program on studies in psychological defense and disinformation.[15] The Swedish Civil Contingencies Agency (MSB) has a popular web course on protecting against influence operations open for anyone,[16] and the Fojo Media Institute at Linnaeus University offers courses for media in disinformation and digital research.[17]

3. *Local Civic Mobilization*

Local municipalities play a vital role in combating disinformation through collaboration with agencies. This political level is closest to the citizens and is also the first responder in times of crisis and war. Some of them, such as Nacka near Stockholm, have started to implement their own educational programs and strategic communication efforts, which also promote awareness in nearby municipalities.[18]

---

14 Government Offices of Sweden, "Mediemyndigheten ges i uppdrag att genomföra nationell satsning för stärkt medie- och informationskunnighet inom AI-driven desinformation [The media authority is tasked with implementing a national initiative for strengthened media and information literacy within AI-driven disinformation]," March 14, 2024, https://www.regeringen.se/pressmeddelanden/2024/03/mediemyndigheten-ges-i-uppdrag-att-genomfora-nationell-satsning-for-starkt-medie--och-informationskunnighet-inom-ai-driven-desinformation/.

15 "Master's program in political science - psychological defense and disinformation," Karlstad University, n.d., https://www.kau.se/en/education/programmes-and-courses/programmes/SAPFD (accessed August 8, 2024).

16 MSB, "Skydd mot informationspåverkan (webbkurs) [Protection against information impact (web course)]," updated November 6, 2024, https://www.msb.se/sv/utbildning--ovning/alla-utbildningar/skydd-mot-informationspaverkan-webbkurs/ (accessed August 8, 2024).

17 "Desinformation och digital research – med EU-vinkel," Fojo Linnaeus University, n.d., https://fojo.se/kurser/desinformation-och-digital-research-med-eu-vinkel/ (accessed August 8, 2024).

18 "Så skyddar vi oss mot informationspåverkan från främmande makt," Nacka kommun, https://www.nacka.se/kommun--politik/trygg-och-saker/beredskapsveckan-2024/sa-skyddar-vi-oss-mot-frammande-informationspaverkan-fran-frammande-makt/ (accessed September 5, 2024).

Swedish businesses and civil society organizations contribute to counter disinformation through various think tanks, commercial training programs, and collaborative efforts with agencies. The labor market organizations in Sweden, both employers and trade unions, work together to counteract disinformation targeted at their members and operations. This had already started in 2018 when all top managements in the umbrella organizations were trained together.[19] Since then, organizations have participated in educational programs to train their members to recognize and handle disinformation. Employer organizations and unions sometimes cooperate with authorities such as the MPF and the National Board of Health and Welfare (NBHW) to counteract disinformation.

4. Security Hardening

Defense and security agencies have been given a clearer role and more resources for countering influence operations, both individually and as a team. Säpo plays a critical role as a security service in identifying and countering influence operations conducted by foreign powers. The agency monitors and analyzes disinformation campaigns, including investigating Swedish citizens who may threaten Sweden's security as agents for foreign powers.

FRA supports the collective defense against influence operations through its signal intelligence capabilities. This enables the detection and identification of communications between foreign actors and their possible agents in Sweden. Much of FRA's capabilities and operations are out of the public's direct sight due to its inherent secrecy, but the Government has in 2022 directed an inquiry to judge whether the rights to direct FRA collection should be extended to MPF.[20]

---

19 "Det demokratiska samtalet i en digital tid," The State's Official Inquiries, SOU 2020:56, https://www.regeringen.se/contentassets/ffa5b8002c4c4913b063bc5862d6fb48/det-demokratiska-samtalet-i-en-digital-tid---sa-starker-vi-motstandskraften-mot-desinformation-propaganda-och-nathat-sou-202056.pdf (accessed August 29, 2024).

20 "Översyn av lagen om signalspaning i försvarsunderrättelseverksamhet," Swedish Government, Dir. 2022:120, https://www.regeringen.se/rattsliga-dokument/kommittedirektiv/2022/07/dir.-2022120 (accessed September 9, 2024).

The Armed Forces has been fighting disinformation in the military field since the early 2000s. The Information Operation section in the Operational Command uses the Armed Forces situational awareness in collaboration with MPF and the Defense Staff's Strategic Communication Department to respond to any malign claims regarding the military situation around the Scandinavian Peninsula.

5. International Collaboration

Sweden has engaged in several international forums to combat disinformation. After Sweden became a member of NATO on March 7, 2024, it has deepened its cooperation in countering disinformation through information exchange, joint planning, and coordinating efforts.

But since 2014, Sweden has been participating in NATO's Interoperability Platform, which brings together allies and selected partners in NATO's crisis management and NATO's Cyber Coalition exercises, which may include scenarios related to disinformation.[21] MSB/MPF have also, in the last decade, seconded personnel to the NATO Strategic Communications Centre of Excellence in Riga.[22]

Sweden collaborates with the EU organ East StratCom Task Force (ESTF), which was organized in 2015 by the European Council within the European External Action Service (EEAS) to address Russia's ongoing disinformation campaigns.[23] In a corollary move, Sweden has also increased its participation in and support of the European Centre of Excellence for Countering Hybrid Threats (Hybrid COE) in Helsinki, Finland, which advances knowledge of hybrid warfare and influence operations' share of an overall effort from

21 NATO, "Relations with Sweden," updated March 28, 2024, https://www.nato.int/cps/en/natohq/topics_52535.htm (accessed September 30, 2024).

22 MPF, "Psychological defence is strengthened within NATO," March 7, 2024, https://mpf.se/psychological-defence-agency/about-us/news/2024/2024-03-07-psychological-defence-is-strengthened-within-nato (accessed August 6, 2024).

23 Euvdisinfo, "Welcome to EUVSDISINFO," n.d., https://euvsdisinfo.eu/ (accessed September 10, 2024).

adversaries using other means than conventional military.[24]

There are also agencies such as the Swedish Institute (SI) which through different collaborations with international partners are promoting Sweden as a country. As part of their mission, they also analyze perceptions and act as an early warning regarding disinformation against Sweden.[25]

6. Regulations

The government has proposed tougher penalties for violence, threats, or insults against public officials to protect those on the front lines against disinformation. The NBHW has received an expanded mandate to counteract rumors and disinformation specifically targeting social services given that the sector has been the target of persistent information manipulation from Islamist actors.

One example is the so-called "LVU-campaign", where Islamist accounts spread systematic disinformation regarding Swedish Care of Young Persons (Special Provisions) Act. The act gives social agencies the mandate to take away children from their parents in case of severe mistreatment threatening the child's health or development. In this campaign, the disinformation sought to portray Swedish authorities as anti-Muslim, which led to threats against social workers across Sweden.[26]

Challenges Ahead Despite Improvements

The above overview suggests that the input of awareness and resources has started to move the wheels in Sweden's society against foreign influence operations. The main question is whether Sweden's strategies to fight foreign influence operations has yielded important outcomes.

---

24 "Hybrid COE, https://www.hybridcoe.fi/.

25 SI, "The image of Sweden abroad 2023," March 2024, https://si.se/app/uploads/2024/03/the-image-of-sweden-abroad-2023.pdf (accessed September 7, 2024).

26 National Defence University, "LVU-kampanjen," 2023, https://www.fhs.se/download/18.32d29dd2187bd01d5e455265/1682576119173/LVU-kampanjen.pdf (accessed August 25, 2024).

A clear result of Sweden's initiatives is the heightened awareness of disinformation among both agencies and the public. The training of civil servants by MSB has improved the public sector's competence in identifying and addressing disinformation campaigns.

The establishment of MPF has enhanced the government's ability to respond to disinformation campaigns, as has the upgrading of collaboration between agencies which has improved their capabilities to react and investigate. In September 2024, the Special Prosecutor for Security Cases announced that he closed a hitherto unknown criminal investigation in collaboration with Säpo, which established that the Iranian Revolutionary Guard in 2023 had hacked a telecom company and sent 15,000 SMS to recipients asking them to send photos of people involved in the burning of Qurans which took place during that period.[27]

The Armed Forces also moved swiftly in September 2024, when Russia claimed that a Swedish SIGINT aircraft was part of an alleged Ukrainian drone attack on Murmansk. In a few hours, the Armed Forces had debunked the story with an effective message and great reach to discredit the disinformation.[28] This was, however, probably only effective for countering the disinformation in Western media. It was likely that the Russian population was the target for this message, and Sweden and its allies have yet to be as effective as possible inside Russia as such disinformation is intended to mobilize the Russian people against perceived foreign enemies.

The editorial media in Sweden has learned rapidly and established some collaboration with colleagues across Europe. This has resulted in several scoops, which is also beneficial to the security authorities as they sometimes get investigative leads from the reporting. The latest example is the work by

27 "Sweden blames Iran for cyber-attack after Quran burnings," *BBC*, September 24, 2024, https://www.bbc.com/news/articles/c0lw0081e1yo (accessed September 30, 2024).

28 Joachim Kerpner, "Ryska medier: "Svenska plan inblandade i drönarattack [Russian media: "Swedish planes involved in drone attack"]," Aftonbladet, September 11, 2024, https://www.aftonbladet.se/nyheter/a/xmMamV/uppgifter-svenska-spaningsplan-vagledde-dronare-mot-rysk-flygplats (accessed September 11, 2024).

TV4, which broke the news regarding a Chinese network in Sweden of 17 individuals trying to influence opinions and, eventually, decisions.[29]

The improved capabilities are a most welcome effect from all the anti- and counter-disinformation efforts of the last decade. However, so have the antagonist's efforts to exploit divisions and create more effective influence operations as can be seen in the Iranian SMS example. There are several challenges ahead for Sweden and democracies at large to combat these operations and strategies.

As the Quran burnings showed, it will be demanding to find a balance between combating disinformation and protecting freedom of speech. This is a complex matter which requires ongoing dialogue and clear guidelines. To separate foreign malicious influence and internal political debate will be particularly delicate as a democracy needs to also be in tune with foreign developments to adapt to changing realities.

The speed of advances in technology is a challenge in identifying disinformation. Manipulated pictures are the most threatening venue of influence as these circumvent reasoning and affect emotions directly. Future measures should include more investment in AI-based detection tools and established sanctions for AI-generated content. It will also be easier in the future to tailor disinformation campaigns to an individual's exposures or vulnerabilities due to the continuous expansion of data on people. Western countries such as Sweden might need to complement the data protection legislation and development of analytical tools to protect against such attack vectors.

Influence campaigns will probably be different in their design and effects for various regions of Sweden, which can be seen as a localization of influence. This means that municipalities and regions may need to act faster and more tailored than the national level can do. Sweden needs to conduct comprehensive studies

29 "Avslöjar: Tillhör hemligt kinesiskt nätverk – som opererar i Sverige [Reveals: Belongs to secret Chinese network - operating in Sweden]," *TV4*, October 1, 2024, https://www.tv4.se/artikel/1TIZeosw51OshC399hNrT8/avsloejar-tillhoer-hemligt-kinesiskt-naetverk-som-opererar-i-sverige (accessed October 1, 2024).

to assess the effects of disinformation across different regions and demographic groups within Sweden. The County boards could be used for knowledge exchange and sharing of best practices amongst the political vertical.

Disinformation campaigns can yield adverse economic repercussions. In 2023, the Minister for Civil Defense, Carl-Oskar Bohlin, voiced concerns that the influence campaign targeting Sweden could jeopardize the security of Swedish citizens and businesses operating abroad.[30] Sweden should, therefore, develop strategies for prompt responses to disinformation threatening Sweden's economic interests.

Despite improvements, there remains a need to bolster media literacy and critical thinking skills among the populace. Increasingly sophisticated disinformation tactics will require regular updating of educational curricula. Education of a larger audience could also come from civil society by initiatives such as Bellingcat.[31]

However, legislation concerning foreign funding of parties or organizations is not being dealt with so far. There are sub-optimal rules in place for financing of political parties and Sweden also does not have a lobby register to increase transparency regarding who are meeting with which legislators. This means that until these circumstances are changed, Sweden is still too susceptible to peer-to-peer influence from nation-states or ideologically motivated actors since there is no scrutiny of which foreign interests that might be promoted.

A heightened cooperation in the "Five Lies-alliance" and augmentation by other states in a loose union to disseminate disinformation against the West underscores a need for enhanced international cooperation. Democracies need to establish capabilities but, more importantly, real-time operational cooperation to reduce the effect of coordinated campaigns.

30 "Increased spread of disinformation directed towards Sweden | Swedish Government | accessed 6 September 2024, https://www.government.se/press-releases/2023/07/disinformation/.

31 Bellingcat. "Home Page," n.d., https://www.bellingcat.com/ (accessed September 8, 2024).

One dimension that is especially absent in contemporary discourse regarding countermeasures is the offensive approach. Based on an analysis of the specific target, Western actors could disseminate *information* into a country to inform a specific subset of the population regarding the actions their regime has conducted and which consequences these choices have.

In Russia, a reasonable target would be the Officer Corps of the Army and the Navy. Suffering horrendous losses during the full invasion of Ukraine partly because the Security Service, FSB, seems to have fed entirely wrong intelligence into the disastrous "Military Special Operation", the surviving officers can be assessed as holding grievances against the FSB and to a lesser extent the Kremlin.[32] Information campaigns could be devised to probe and possibly exploit such feelings to achieve outcomes such as indifference towards the regime, animosity towards the FSB, and ultimately demands of restructuring the combat power of the Russian Federation or, in effect, a decrease of the combat power through disunity.

As another example, Iran has a large part of the population which is resistant to the regime, and there is also a rather large and successful diaspora with the same attitude and excellent reach into Iran. EU and/or NATO could contemplate whether it would be beneficial to inform these groups that sanctions will be expanded so as to make the Iranian regime change their calculus of conducting divisive influence operations in democracies. Each opponent needs a tailored counterstrategy from the West to be effective.

Sweden still needs to articulate an overall strategy to defeat foreign influence operations, develop and improve critical capabilities and with allies become more assertive in order to take back the initiative from Western opponents. That journey has just begun.

---

32 Greg Miller and Catherine Belton, "Russia's spies misread Ukraine and misled Kremlin as war loomed," Washington Post, August 19, 2022, https://www.washingtonpost.com/world/interactive/2022/russia-fsb-intelligence-ukraine-war/ (accessed September 8, 2024).

4. Russia's Resilient Disinformation Machine

Ilan Berman

Though it is only comparatively recently that Russian disinformation has re-emerged in the contemporary public consciousness, the phenomenon itself is far from new.[1] Rather, it is a practice with a long history, dating back to *tsarist* times, as well as a distinct strategic purpose. Over the decades of the Cold War, it served as one of the most enduring and effective tools of Soviet asymmetric warfare against the West. And in the post-Cold War era, it has become a core element of foreign policy for the government of Vladimir Putin, helping to buttress and empower the Kremlin's neo-imperial impulses.

Today, moreover, both the volume and the effectiveness of Russian disinformation is growing. Russian fake news and propaganda are being amplified by a new, more crowded global informational environment in which traditional sources of news and opinion are being increasingly challenged by new (and often unreliable) information outlets and social media platforms. This altered media terrain has provided the Kremlin's propagandists with fresh opportunities to disseminate divisive tropes, undermine the authority of the Western-led liberal order, and posit an alternative vision of the world more consonant with Moscow's increasingly assertive, revisionist worldview.

A Persistent Strategy

At its core, Russian information manipulation is rooted in the country's unique conception of war and peace—one that is fundamentally different from that

1 This chapter is drawn in part from Ilan Berman, *Challenging Moscow's Message: Russian Disinformation and the Western Response* (AFPC Press, 2023).

which is collectively held by the nations of the West.[2] In Europe and the United States, officials and policymakers overwhelmingly view war and peace as fundamentally different and opposing concepts. Either one prevails, or the other does. In Russia, by contrast, war and peace have long been viewed as part of the same continuum, with emphasis placed on techniques, tactics, and strategies that could confer advantage on the Kremlin in a competitive process that could, conceivably, culminate in warfare.

As a result, beginning in the 1950s, the Soviet Union placed significant emphasis on the development of techniques for influencing foreign behavior short of war. This field, broadly known as "active measures" (*aktivniye meropriyatiya* in Russian), quickly became the Kremlin's main strategy to shape events and policy in other countries.[3] In fact, defectors have divulged, "active measures"—rather than traditional intelligence gathering activities—occupied the lion's share of attention and resources on the part of the KGB, the Soviet Union's main foreign intelligence agency, during the decades of the Cold War.[4]

Of the different tactics employed as part of Soviet "active measures," disinformation (*dezinformatsiya* in Russian) was among the most effective, designed to weaken adversaries through information manipulation. Soviet disinformation, the scholars Richard Schultz and Roy Godson have noted, was used "to strengthen allies and weaken opponents and to create a favorable environment for the achievement of Soviet foreign policy objectives." As a result, they were "systematically and routinely conducted on a worldwide scale."[5]

---

2 Stephen J. Blank, ed., *The Russian Military in Comparative Perspective* (U.S. Army War College, 2016), https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=1910&context=monographs.

3 C.W. Bill Young, "Soviet Active Measures in the United States – An Updated Report by the FBI," *Congressional Record* E 4716, December 9, 1987, https://www.cia.gov/readingroom/docs/CIA-RDP11M01338R000400470089-2.pdf.

4 G. Edward Griffin, "Soviet Subversion of the Free-World Press: A Conversation with Yuri Bezmenov," 1985, https://www.youtube.com/watch?v=pOmXiapfCs8.

5 Richard H. Shultz and Roy Godson, *Dezinformatsiya: Active Measures in Soviet Strategy* (Pergamon-Brassey's, 1984), 2.

With the Soviet collapse, Russia's use of disinformation temporarily diminished as the country underwent massive internal changes. For a time, at least, it appeared that the once all-powerful Soviet KGB would be dismantled and undergo a reduction of its strength and influence. Comparatively quickly, however, real efforts to reform the Soviet Union's premier intelligence agency faltered, and by the mid-1990s a process of reconsolidation was underway—one in which the KGB, now rebranded the FSB, regained both power and authority. Russian disinformation charted a similar trajectory. The breakup of the Soviet Union in 1991, followed by the chaos of Russia's short-lived experiment with democratization during the 1990s, offered at least a brief reprieve from the Kremlin's use of deception and subversion against its international adversaries. But, parallel with the resurgence of the Soviet-era intelligence state, disinformation experienced a revival, as Russia's new rulers once again made it a core part of their foreign policy and intelligence operations.

Given Russian President Vladimir Putin's early career as a KGB agent, it was perhaps inevitable that his regime would come to rely heavily on one of the agency's most potent Soviet-era tactics. Less than a year after Putin assumed the Russian presidency in late 1999, the Kremlin issued a foreign policy and information doctrine laying out that the country faces an array of threats in the information domain, requiring "stepping up counter-propaganda activities."[6] A decade later, Russia's 2010 defense doctrine formally authorized the use of information warfare to proactively shape the global order, and to condition the international environment to the subsequent use of military force.[7] And the 2021 *National Security Strategy of the Russian Federation* identifies "information security" as a core area of concern, and emphasizes the importance of the "development of forces and means of information confrontation."[8]

---

6 Russian Federation, *Information Security Doctrine of the Russian Fe*deration, 2000, https://base.garant.ru/182535.

7 The Kremlin, "Military Doctrine of the Russian Federation," February 5, 2010. An English language translation is available at https://carnegieendowment.org/files/2010russia_military_doctrine.pdf.

8 President of the Russian Federation, *Strategia Natsionalnoye Bezopastnostii Rosiyskoy Federatstii* [National Security Strategy of the Russian Federation], July 2, 2021, http://actual.pravo.gov.ru/text.html#pnum=0001202107030001.

In the service of this priority, the Russian state has erected an elaborate informational architecture, encompassing state-run television and multimedia channels, news agencies, web- and social media-based messaging outlets, stakes in foreign newspapers and television channels, as well as proxy actors (like the infamous Internet Research Agency).[9] Through this ecosystem, Russia has managed to create what scholars have termed a "firehose of falsehood" that it uses to obscure objective truth, outshout and outmaneuver legitimate news sources, and advance its own version of world events through "high-volume, multichannel, and continuous messaging."[10]

This enterprise enjoys enormous resources. As of early 2023, and despite the heavy economic toll of the Ukraine war and the impact of widening Western sanctions, European officials still estimated the Kremlin to be spending some USD 2.4 billion annually on disinformation and propaganda activities.[11]

Modern Appeal

What makes Russian disinformation so effective, both at home and abroad? The question is apt, given the course of Russia's current war of aggression against Ukraine, and the heavy losses (both economic and human) that the country has incurred as a result. The answer can be traced back to several factors.

Internally, demographics play a significant—if underappreciated—role. Russia, after all, has been on a trajectory of protracted population decline for more than half a century, and that downward trend was significantly exacerbated by the Soviet collapse.[12] While it has fared a bit better in more recent years, the pace of the Russian population—estimated at approximately 1.4 as of

9 For a detailed examination, see Berman, *Challenging Moscow's Message*, 21-24.

10 Christopher Paul and Miriam Mathews, "The Russian 'Firehose of Falsehood' Propaganda Model: Why It Might Work and Options to Counter It," Rand Corporation *Perspective* no. 198, 2016, https://www.rand.org/pubs/perspectives/PE198.html.

11 Author's interview with NATO strategic communications specialist, Riga, Latvia, February 2023.

12 World Bank, "World DataBank: World Development Indicators," n.d., available athttp://databank.worldbank.org/data/reports.aspx?source=2&country=&series=SP.DYN.TFRT.IN&period=#.

mid-2024[13]—remains well below the total fertility rate of 2.1 required for a sustainable replenishment of the state. It is also stubborn, having remained largely static despite numerous policies adopted by the Kremlin with the aim of ameliorating the national population decline.

While the drivers of Russia's demographic downturn are manifold, emigration has played a decisive role. When measured in 2021, approximately five million people were estimated to have fled Russia in the two decades since Vladimir Putin took power.[14] Moreover, this dynamic has been greatly exacerbated by the current war in Ukraine, which has precipitated the largest exodus of Russians from the country since the 1917 Bolshevik Revolution.[15]

Notably, this trend is not value-neutral. Rather, it has been heavily weighted toward what demographer Judy Twigg has termed the "creative class"—that is, "scientists, educators, artists and knowledge-based workers" who have left Russia in order to escape deepening authoritarianism and a stifling intellectual climate.[16] They have left behind a Russian population that is generally less mobile, less educated and more susceptible to the extensive state-promoted propaganda that pervades virtually every aspect of contemporary Russian life, from education[17] to entertainment.[18] This helps to explain why, despite the heavy economic and

13 See, for instance, "'Disastrous' Russian birth rate putting country's future at risk, Kremlin says," *Agence France-Presse*, July 27, 2024, https://www.scmp.com/news/world/russia-central-asia/article/3272093/disastrous-russian-birth-rate-putting-countrys-future-risk-kremlin-says.

14 As cited in Uliana Pavlova, "5 Million Russian Citizens Left Russia under Putin," *The Moscow Times*, October 13, 2021, https://www.themoscowtimes.com/2021/10/13/5-million-russian-citizens-left-russia-under-putin-a75246.

15 Francesca Ebel and Mary Ilyushina, "Russians abandon wartime Russia in historic exodus," *Washington Post*, February 13, 2023, https://www.washingtonpost.com/world/2023/02/13/russia-diaspora-war-ukraine/.

16 Judy Twigg, "Russia is Losing its Best and Brightest," *The National Interest*, June 13, 2016, http://nationalinterest.org/feature/russia-losing-its-best-brightest-16572.

17 Howard Amos, "Russian Schools Are Teaching 3-Year-Olds Propaganda about the War in Ukraine," Vice, March 25, 2022, https://www.vice.com/en/article/russia-ukraine-war-propaganda/.

18 See, for instance, "Pro-Kremlin Pop Star's Concert a Microcosm of Russia's Wartime 'Patriotism,'" *The Moscow Times*, September 10, 2023, https://www.themoscowtimes.com/2023/09/10/pro-kremlin-pop-stars-concert-a-microcosm-of-russias-wartime-patriotism-a82414.

human toll of his war of choice, Vladimir Putin appears to continue to enjoy comparatively high levels of support—although the increasingly repressive nature of the Russian state makes polling there notoriously unreliable. At a minimum, however, the Ukraine war has not yet engendered the type of grassroots discontent that could imperil Putin's hold on power. For that, the Kremlin's pervasive domestic propaganda is significantly responsible.

Externally, meanwhile, Russian propaganda is tailored to diminish the authority and appeal of the West. Unlike the informational efforts of China, which focus overwhelmingly on "telling good stories" about the PRC to global audiences,[19] Russia is relaying a qualitatively different narrative. Unlike Beijing, Moscow is not attempting to sell its own model of governance to the world. Rather, its informational efforts are intended to advance its geopolitical objectives by diminishing global support for its adversaries, and lessening resistance to its own preferences.

In this, Russian disinformation has been greatly aided by recent changes in global media, from the proliferation of social media platforms to the rise of new technologies, such as artificial intelligence, that have made information manipulation and the dissemination of Russian narratives much easier. Kremlin-aligned disinformation actors have been deftly exploiting these changes to gain greater resonance for their messaging and to reach new audiences. To this end, recent years have seen the Kremlin make major investments in the expansion of its media outreach beyond its traditional ambit of the *Russkiy Mir* (Russian world) and Europe, into the developing world.

In Latin America, for instance, Russia is now operating a formidable media enterprise (consisting of multiple broadcast networks, social media messaging, and propaganda) that outstrips U.S. media engagement in the scope and breadth of its outreach toward regional states, experts say.[20] In Africa, meanwhile,

---

19 Joshua Eisenman, "China's Media Propaganda in Africa: A Strategic Assessment," United States Institute of Peace Special Report, March 16, 2023, https://www.usip.org/publications/2023/03/chinas-media-propaganda-africa-strategic-assessment.

20 Interview with Joseph Michael Humire, *AFPC Disinformation Wars podcast*, episode 27, December

the Russian government and its proxies have been carrying out a "massive disinformation campaign" shifting the blame for rising global food and energy prices to the West in an effort that is "intended to both hide Russia's culpability and persuade leaders of at-risk countries to support an end to sanctions designed to stop Russia's unjust and brutal war in Ukraine."[21] And in the Middle East, Russia is waging a "disinformation war" to shape regional opinion, amplifying false narratives and conspiracy theories via Arabic-language social media outlets and pushing its own propaganda via state-owned media channels, all of which boast Arab-language programming.[22]

This approach has proven markedly effective. While in the United States and Europe, opposition to Russia's war of aggression against Ukraine is widespread, Moscow is making major gains in advancing its position—and eroding that of the West—throughout the developing world, thanks to its propaganda and messaging capabilities. Thus, the 2023 edition of the Democracy Perception Index, the world's largest annual study on democracy, found a wide gap between Western attitudes toward Russia and those of countries in the "Global South," including Mexico, Malaysia, Algeria, and Nigeria, where a much more favorable view of Moscow continues to predominate.[23]

An Ominous Convergence

Russian disinformation is not a singular enterprise. While Russia has unquestionably been a pioneer in the weaponization of information, recent years have seen other countries surge forward in their strategic use of

22, 2022. https://podcasters.spotify.com/pod/show/afpcdisinfowarfare/episodes/EPISODE-27-Russiandisinformation-is-helping-reshape-Latin-America-e1sjilf/aa937q9g.

21 U.S. Department of State, Global Engagement Center, "Russia's Disinformation Campaign Cannot Hide its Responsibility for the Global Food Crisis," June 22, 2022, https://www.state.gov/disarming-disinformation/russiasdisinformation-cannot-hide-its-responsibility-for-theglobal-food-crisis/.

22 See, for instance, H.A. Hellyer, "Russia is waging a disinformation war in the Middle East," *Politico Europe*, April 7, 2023, https://www.politico.eu/article/vladimirputin-sputnik-rt-russia-is-waging-a-disinformation-war-inthe-middle-east/.

23 Latana/Alliance of Democracies, *Democracy Perceptions Index 2023*, May 2023, https://6389062.fs1.hubspotusercontent-na1.net/hubfs/6389062/Canva%20images/Democracy%20Perception%20Index%202023.pdf.

information operations. Authoritarian states such as China, Iran, Turkey, and Qatar have charted significant advances in the manipulation of media and informational narratives. So, too, have extremist groups such as the Islamic State, capitalizing upon a media environment in which the barriers for entry have been dramatically lowered.[24]

These actors, moreover, are increasingly benefiting from Russia's acumen in the manipulation of information. Thus, amid growing strategic cooperation between Russia, China, and Iran in recent years, the Kremlin's propaganda and information manipulation playbook has increasingly been embraced in both Beijing and Tehran in a process which experts have termed "authoritarian learning."

The past several years have provided ample evidence of such collaboration. At the height of the coronavirus pandemic, for instance, the European Union's European External Action Service (EEAS) assessed that Russian disinformation about COVID-19 was being taken up and amplified by both China and Iran in what amounted to a "trilateral convergence of disinformation narratives" aimed at sowing confusion and diminishing trust in the West among global audiences.[25] So extensive was this collaboration that some authors termed it an "axis of disinformation."[26] More recently, false Russian narratives about Ukraine, formulated in support of the Kremlin's "special military operation" against Kyiv, have been echoed by China as part of the so-called "no limits" partnership between Russia and the PRC.[27]

---

24 For a detailed examination of this phenomenon, see Ilan Berman, ed., *Digital Dictators: Media, Authoritarianism, and America's New Challenge* (Rowman & Littlefield, 2018).

25 Rikard Jozwiak, "EU Monitors See Coordinated COVID-19 Disinformation Effort by Iran, Russia, China," *Radio Free Europe/Radio Liberty*, April 22, 2020, https://www.rferl.org/a/eu-monitors-sees-coordinated-covid-19-disinformation-effort-by-iran-russia-china/30570938.html.

26 Andrew Whiskeyman and Michael Berger, "Axis of Disinformation: Propaganda from Iran, Russia, and China on COVID-19," Washington Institute Fikra Forum Policy Analysis, February 2021, https://www.washingtoninstitute.org/policy-analysis/axis-disinformation-propaganda-iran-russia-and-china-covid-19.

27 See, for instance, David Bandurski, "China and Russia are joining forces to spread disinformation," Brookings Institution, March 11, 2022, https://www.brookings.edu/techstream/china-and-russia-are-joining-forces-to-spreaddisinformation/.

As these examples, and countless others, demonstrate, Russia's expertise in manipulating the information space has begun to enhance the respective disinformation enterprises of like-minded authoritarians. As a result, the United States and its partners in the West will face a more sophisticated, multifaceted, and hostile informational environment in the years ahead.

This adversarial manipulation of the information space, moreover, is set to become a key battleground in the unfolding "great power competition" that has become the central organizing principle undergirding the national security agendas of successive administrations in Washington. That makes Russia's manipulation of the information sphere an enduring challenge for the United States and its international partners—and raises the importance of erecting effective, collaborative informational strategies to counter it. For both Washington and the broader West, it is long past time to begin.

5. Prospects for Sino-Russian Collaboration: Shared Interests and Strategic Objectives in Disinformation Campaigns

Shiaushyang Liou

Since the establishment of a "Strategic Partnership of Coordination" in 1996, Sino-Russian relations have continuously strengthened. After signing the Treaty of Good-Neighborliness and Friendly Cooperation in 2001, the two countries further enhanced their relationship in 2011, forming a "Comprehensive Strategic Partnership of Coordination," which was elevated again in 2019 to a "Comprehensive Strategic Partnership of Coordination for a New Era." The continued warming of Sino-Russian relations is closely tied to the post-Cold War international landscape. Since the mid-1990s, China and Russia have consistently advocated anti-hegemony and a multipolar international system, with their primary target being the U.S. Russia seeks to regain the superpower status it held during the Soviet era, while a rising China is eager to expand its global influence, including the reunification of Taiwan. Both China and Russia share a strategic goal of pursuing superpower status, with their common obstacle being the world's current sole superpower—the U.S. In other words, China and Russia share common interests in countering the U.S.

Although great powers may not easily resort to war, China and Russia have been employing every possible means to achieve their strategic objectives. Non-military tactics such as disinformation and cognitive warfare, which are low-cost and highly effective, have become their preferred tools. This explains why Russia interfered in the 2016 and 2018 U.S. presidential elections,

while China, during its "Great External Propaganda" campaign, also used disinformation to infiltrate and divide its adversaries. This chapter will first analyze the nature of Sino-Russian relations, then explore the role of disinformation campaigns in their cooperation, and finally assess the prospects for Sino-Russian collaboration.

Sino-Russian Relations: An Axis of Expediency

On February 24, 2022, Russia launched its "Special Military Operation" in Ukraine, and Sino-Russian relations reached a new high just before the war. Russian President Vladimir Putin visited China on February 4 under the pretext of attending the Winter Olympics, and the two nations issued a joint statement declaring that their "friendship has no limits, and their cooperation has no forbidden areas."[1] However, as the Russian military's progress did not meet expectations and failed to capture Kyiv in a blitzkrieg, China's stance became more reserved. In an interview on Phoenix TV's program "Talk with World Leaders" on March 20, 2022, then-Chinese Foreign Minister Qin Gang emphasized that while Sino-Russian cooperation has no forbidden areas, it does have red lines. He further noted that current Sino-American relations were already troubled enough, and China did not wish for the Ukraine crisis to cause further damage to their relationship.[2]

As the war became a stalemate, China's attitude toward the Russo-Ukrainian War shifted to neutrality, urging both sides to negotiate peace. However, China's actions have been inconsistent with this neutrality. Besides importing Russian energy and raw materials, China has also provided dual-use materials to Russia. Strategic coordination between China and Russia, such as high-level visits, strategic-level exercises, joint military drills, joint naval patrols, and joint air strategic patrols, has not ceased due to the Russo-Ukrainian War. In March 2023, China and Russia further declared their intent to deepen their

1 "Joint Statement of the Russian Federation and the People's Republic of China on International Relations Entering a New Era and Global Sustainable Development (in Russian)," President of Russia, February 4, 2022, http://www.kremlin.ru/supplement/5770.

2 "Transcript of Qin Gang's interview with Phoenix TV's 'Wind and Cloud Dialogue' program on March 20 (in Chinese)," Phoenix TV, March 27, 2022, https://news.ifeng.com/c/8GcPIcN27RK.

"Comprehensive Strategic Partnership of Coordination for a New Era." It is evident that China's neutrality is only superficial, as it continues to covertly support Russia while avoiding triggering secondary sanctions from the U.S.

Being isolated by the West, Russia has no other option but to "pivot to the East." Therefore, Russia hopes even more for China to make a public statement, and as a result, continuously seizes opportunities to disclose China's private support. For example, on September 8, 2022, Li Zhanshu, then Chairman of the Standing Committee of the National People's Congress of China, paid a visit to the State Duma, the lower house of Russia's Parliament. In its English-language press release, the State Duma highlighted that Li assured China's understanding and support on issues of vital interest to Russia, particularly regarding the situation in Ukraine. Li emphasized that China fully understands Russia's need to take all necessary measures to protect its key interests and is providing support accordingly.[3] A video of Li's closed-door meeting with the State Duma members was later leaked. In the video, Li's remarks were generally consistent with the content of the State Duma's press release. However, his statement that "China understands and supports [Russia] and provides '策應' (coordination) in various ways"[4] sparked an immediate public outcry after it was revealed. This was because the Chinese term "策應" can mean "two armies responding to each other and coordinating in battle," which is far more intense than the usual meaning of assistance.

A similar scenario occurred on January 31, 2024, during a video conference between China's new National Defense Minister, Dong Jun, and former Russian Defense Minister Sergey Shoigu. Dong's remarks were reported by Russia's TASS news agency, where he stated, "We provide support to you on

3 "Leaders of the State Duma factions met with Chairman of the Standing Committee of the National People's Congress," The State Duma, The Federal Assembly of the Russian Federation, September 9, 2022, http://duma.gov.ru/en/news/55208/.

4 "Li Zhanshu: On issues involving Russia's vital interests, especially the situation in Ukraine, China understands and supports and provides support from different aspects (in Chinese)," Epoch TV Chinese Station, September 14, 2022, https://x.com/EpochTV_CH/status/1570029219178024961.

the Ukraine issue. Despite continuous pressure from the U.S. and Europe and even attacks on China-EU defense cooperation, we will not change or abandon our established policy. They should not, and cannot, interfere with the normal cooperation between Russia and China."[5] Dong's statement appears to be the first time China has explicitly acknowledged its support for Russia in the Russo-Ukrainian War. However, this statement was not published on the website of China's Ministry of National Defense or reported by Chinese state media. This suggests that while the ongoing war in Ukraine involves Russia's core national interests, China, considering its own national interests, is still carefully avoiding becoming entangled in the conflict, let alone sending troops to Ukraine to assist Russian forces. Similarly, even though the Taiwan issue concerns China's core national interests, Russia has so far only expressed verbal support. Despite the increasing intensity and scope of Sino-Russian joint air and naval patrols in recent years, there has been no concrete action specifically targeting Taiwan.

In areas of shared interest, such as opposing U.S. hegemony, advocating for a multipolar world, criticizing NATO and the U.S., promoting Arctic development, opposing unilateral pursuits of absolute security and advocating for global missile defense systems, and supporting the implementation of local currency settlement, China has no hesitation in supporting Russia. After all, these issues do not directly harm China's own interests. However, once it touches on the core interests of the other party and potentially threatens its own interests, China and Russia would respond differently. Indeed, both countries are unwilling to become embroiled in conflicts unrelated to their own interests due to the other's mistakes.

There are also precedents where each country has chosen to remain detached in crucial moments. For instance, during the 2008 Russo-Georgian War, China remained neutral, while Russia avoided involvement in China's border disputes with India. Russia's neutrality in the South China Sea disputes and

5 "China will not abandon its support for Russia on the Ukrainian issue, despite US pressure (in Russian)," TASS, January 31, 2024, https://tass.ru/mezhdunarodnaya-panorama/19864301.

China's lack of support for Russia's annexation of Crimea further highlight this pattern. It is also unlikely that Russia would provide direct military assistance to China in resolving the Taiwan issue. Therefore, China's shift to a neutral stance after discovering Russia's failure to achieve quick success in Ukraine and its call for peace talks comes as no surprise. According to Article 9 of the Sino-Russian Treaty of Good-Neighborliness and Friendly Cooperation, when either party faces threats to peace or aggression, they must consult with each other.[6] Although the treaty does not specify how to handle threats, there is external skepticism that China and Russia intentionally leave room for a military alliance, which allows both countries to retain flexibility in interpretation and decide on subsequent responses. Therefore, Sino-Russian relations can be described as a quasi-alliance without obligatory burdens, with activation depending on the willingness of both parties.

This is why Sino-Russian relations have been characterized as an "axis of convenience," driven more by pragmatism and opportunism rather than by shared values or long-term commitments.[7] In light of current circumstances, describing Sino-Russian relations as an "axis of expediency" is clearly more fitting, as the cooperation between China and Russia is based on expedient considerations rather than deep-seated consensus or long-term commitment, with a stronger emphasis on strategic and temporary factors.

Disinformation Campaigns Facilitate Sino-Russian Strategic Convergence

Despite the expedient nature of Sino-Russian relations, the current international reality leaves the two countries with little choice but to cooperate. Neither China nor Russia can achieve their strategic goals of becoming superpowers on their own. Moreover, within the context of the triangular relationship between

6 "Treaty on Good-Neighborliness, Friendship and Cooperation between the Russian Federation and the People's Republic of China (in Russian)," Ministry of Foreign Affairs of the Russian Federation, July 18, 2001, https://www.mid.ru/web/guest/maps/cn/-/asset_publisher/WhKWb5DVBqKA/content/id/576870.

7 Bobo Lo, *Axis of Convenience: Moscow, Beijing, and the New Geopolitics* (London: Chatham House, 2008), 3.

the U.S., Russia, and China, both China and Russia have shared interests in countering the U.S. Aside from each other, neither country has a better alternative for collaboration. However, the expedient nature of Sino-Russian relations remains a challenge to deeper cooperation, mainly due to their divergent core national interests, which are shaped by geographical politics. China's core national interests lie in the Asia-Pacific region, while Russia's core national interests lie in Europe. Geographic and capability limitations and a lack of willingness mean that China and Russia have consistently approached their cooperation based on pragmatic considerations.

Nevertheless, in the digital age, disinformation campaigns can potentially mitigate some of the geopolitical divergences between China and Russia and even ease the inherent expediency in their relationship. For a Sino-Russian strategic partnership focusing more on rights than responsibilities, disinformation campaigns—offering significant strategic impact at a low cost—are an ideal tool. As long as these efforts do not harm their own interests, the likelihood of limitless Sino-Russian cooperation increases. Although China, constrained by international realities and national interests, ignored the previously declared limitless strategic partnership with Russia and did not dispatch troops to Ukraine to support the Russian military, it later engaged in spreading misinformation about the Russo-Ukrainian War both domestically and internationally. To some extent, this helped to make up for the strategic partner obligations it had not fulfilled earlier. For example, during the first 100 days of Russia's invasion of Ukraine, China echoed Russian narratives at low cost, contributing to a shared theme in Sino-Russian information spaces: anti-Americanism, anti-Western sentiment, and portraying Russia as both victim and hero.[8]

Later, Chinese media continued to amplify Russian viewpoints but shifted its focus to portraying China as the "hero" advocating peace talks and the

8 Asia Fact Check Lab, Detector Media, Doublethink Lab, and IRI Beacon Project, "One Hundred Days of the Invasion of Ukraine: A Comparative Analysis of Sino-Russian War Narratives (in Chinese)," *Radio Free Asia*, https://www.rfa.org/cantonese/news/factcheck/first-100-days-full-report-chn-traditional.pdf.

U.S. as the "villain" fueling the conflict. The Chinese Foreign Ministry frequently used terms like "promoting peace talks" and "fanning the flames" when discussing the Russo-Ukrainian War, applying similar rhetoric to the Taiwan Strait situation by accusing the U.S. of stoking tensions. China's official statements were relatively restrained, while its state media amplified false narratives, creating a division of labor. China's disinformation approach toward the Russo-Ukrainian War has exhibited both consistency and variation.

The consistent aspect is the alignment of Chinese media narratives with Russian viewpoints, while the variation lies in the evolving portrayal of China's role. Initially, China maintained a façade of neutrality but gradually shifted to positioning itself as an active promoter of peace.[9] China naturally avoids engaging in actions that are not beneficial to itself. In its narrative, the U.S. is portrayed as the instigator of both the Russo-Ukrainian war and the Taiwan Strait issue, being the greatest obstacle to peace and responsible for the worsening of all situations. Russia is depicted as a victim forced into war, while China is portrayed as a peacemaker advocating for negotiations between the parties. In this disinformation campaign, China not only addresses its strategic partner Russia but also takes the opportunity to enhance its own image, aiming to make the international community perceive it as a responsible great power and a peace promoter.

Russia has similarly engaged in disinformation campaigns, especially targeting Taiwan. Although Taiwan is not deemed a major issue in Russia, pro-Kremlin Telegram accounts seized the opportunity of the 2024 Taiwanese presidential election to question Taiwan's sovereignty. According to research by the Doublethink Lab, Russian disinformation tactics concerning Taiwan follow three main models. First, they frame any political victory by the Democratic Progressive Party (DPP) or Kuomintang (KMT) as a result of U.S. or Chinese manipulation, implying that Taiwan is a battleground between the U.S. and China. Second, they blame the U.S. as the provocateur and instigator

9 Zhuang Jing, "Over the past year since the Russo-Ukrainian war, how has China told war stories? (in Chinese)," *Radio Free Asia*, May 8, 2023, https://www.rfa.org/cantonese/news/factcheck/100dayreport-05082023091045.html.

of conflicts, claiming that a DPP victory would lead to more American weapons and military facilities in Taiwan, making war in the Taiwan Strait inevitable. They portray the U.S. as using Taiwan to serve its own geopolitical interests. Third, they question the legitimacy of Taiwan's democratic election, oversimplifying voter preferences and suggesting that a majority of Taiwanese support closer ties with China. This narrative also includes magnifying instances of communication failures to imply election interference by the ruling authorities.[10]

For those unfamiliar with Taiwan's political landscape, these disinformation operations may seem plausible, but their content is actually far from the truth. Labeling Taiwan's political parties—equating the DPP with American interests and the KMT with Chinese ones—oversimplifies the complexities of Taiwan's internal politics. Furthermore, the accusations that Taiwan might launch aggression against China, that the DPP might further arm the island and demonize Beijing, and even the suggestion that China should negotiate with the KMT stronghold of Miaoli County on Taiwan's western coast for amphibious military operations, are largely exaggerated speculations. In reality, Taiwan's strategy is to prepare for defense, not war, especially given the stark military imbalance with China. China, through its gray zone tactics, is the true provocateur.

As for China's efforts to manipulate Taiwan's local governments for potential military operations, such strategies are more aligned with fictional narratives rather than actual geopolitics. In truth, Taiwan poses no threat to Russia, and its economy could complement Russia's with competitive Taiwanese products such as 3C electronics and precision machinery tools. There is no real reason for Russia to demonize Taiwan. The disinformation spread by pro-Kremlin accounts on Telegram is primarily aimed at undermining the U.S. and indirectly aiding China. For example, casting doubt on Taiwan's democratic elections, fostering divisions within Taiwanese society, and framing the

10 Levi Bochantin, "How Russia's Telegram Shaped Taiwan's Election and Subjectivity Issues (in Chinese)," Taiwan Democracy Laboratory, June 3, 2024, https://medium.com/doublethinklab-tw/俄羅斯-telegram-如何形塑台灣大選與主體性議題-253bd6fde481.

election and the future Taiwan Strait conflict as a proxy war between the U.S. and China ultimately serve the purpose of weakening American influence. Otherwise, given Taiwan's harmlessness to Russia, these pro-Kremlin actors wouldn't need to go to such great lengths.

Although the disinformation campaigns by China and Russia on online media platforms may seem absurd, they still help both countries target their common adversary, the U.S., and achieve their strategic goal of becoming superpowers. Assistance to their partner is a secondary, incidental effect. Moreover, due to geographical and capability constraints, it is currently impractical for China and Russia to deploy troops to fight on each other's behalf for their core national interests. In this context, low-cost and high-benefit disinformation campaigns are the best option. While they cannot replace tangible military actions, they still contribute to Sino-Russian strategic convergence. However, the performance of their disinformation campaigns reflects the expedient nature of their cooperation and the instability of their relationship. The Sino-Russian expedient axis is a combination where the tighter the cooperation, the more apparent the contradictions become. At present, they have temporarily set aside their differences in the face of a common adversary, the U.S.

Conclusion

The rapid enhancement of the Sino-Russian strategic partnership after the Cold War is closely related to the U.S., which acts as a barrier to both China and Russia's ambitions to become superpowers. To achieve this strategic goal, China and Russia share a common interest in countering the U.S. In reality, the Sino-Russian relationship is an expedient axis; their cooperation is based on expedient considerations rather than deep-seated consensus or long-term commitment. This has been fully revealed in the recent Russo-Ukrainian War. Even though the war involves Russia's core national interests, China has disregarded the Sino-Russian strategic partnership and the pre-war declaration of "unlimited cooperation." Instead, China has adjusted its stance according to the developments of the war, ultimately adopting a position of apparent neutrality while secretly aiding Russia to avoid direct involvement in the conflict. In fact, when issues touch upon China's core national interests, such

as the Taiwan issue or the South China Sea issue, Russia also adopts a neutral observer stance to avoid becoming involved. Both countries are unwilling to become embroiled in conflicts that are unrelated to their own interests due to the other's mistakes.

The expedient nature of the Sino-Russian relations is not conducive to their cooperation. This is largely due to China and Russia's differing core national interests, which are rooted in geopolitical factors. China's core national interests lie in the Asia-Pacific region, while Russia's core national interests are in Europe. Geographical and capability constraints, combined with a lack of willingness, result in both countries consistently approaching their cooperation from an expedient perspective. For the Sino-Russian strategic partnership, which only talks about rights but avoids obligations, disinformation campaigns with relatively low costs compared to tangible military operations may eliminate some of the geopolitical divergences between the two countries and even mitigate a degree of expediency. This makes disinformation campaigns the preferred means for achieving maximum benefit at minimal cost. After all, as long as it does not harm their own interests, the possibility of limitless cooperation between China and Russia increases. Therefore, China continuously repeats the Russian narrative of the Russo-Ukrainian War, shaping anti-American and anti-Western sentiments while portraying Russia as a victim and hero. China also uses this opportunity to present itself as a peacemaker advocating for dialogue, while the U.S. is depicted as the biggest obstacle to peace, fueling the Russo-Ukrainian War and even the Taiwan Strait issue. Similar tactics are seen in Russia as well. The Taiwan presidential election and the Taiwan Strait issue are portrayed as a struggle between China and the U.S., with the U.S. being held responsible for the Taiwan Strait issue. The Taiwan presidential election is even falsely presented as an unjust election that does not reflect true public opinion, creating the illusion that most Taiwanese actually wish to strengthen ties with China.

The fact that China and Russia are only willing to engage in disinformation campaigns on issues that do not directly affect their own interests but involve the core national interests of the other party and are not pursuing tangible

military operations that could alter the status quo despite their strategic partnership and the declaration of "unlimited cooperation," one can see their expedient considerations. Moreover, the disinformation campaigns reveal that the primary goal of both countries is to target their main adversary, the U.S., with any benefit to their partner being a secondary effect. In other words, whether something is beneficial to themselves is the main consideration, while the benefit to their partner is secondary. Therefore, the prospects of Sino-Russian cooperation, which are fundamentally expedient, are not optimistic. Even though disinformation campaigns help mitigate the expedient nature of Sino-Russian relations, they are merely a temporary solution rather than addressing the root of the issue.

6. Sino-Russian Disinformation Cooperation in Nordic Countries: Interests, Prospect & Mitigation

Jeanette Serritzlev

The aim of this chapter is to examine the prospect of a closer Sino-Russian cooperation in the field of disinformation. While other chapters address the disinformation means and strategies of the two state actors in depth, this chapter only scratches the surface in order to set the context. Outlining the mutual interests between the two state actors, the chapter attempts to picture, how such a further cooperation could look like in the Nordic region. Likewise, the author will address limitations of such a cooperation due to divergent strategic interests. Finally, the chapter will discuss how the Nordic countries can mitigate and protect themselves against such a scenario.

PRC & Russia: Mutual Interests and Divergent Strategic Interests

The NATO Summit Declaration from July 2024 addresses the growing concern from a Western point of view of the increasingly growing cooperation between Russia and the PRC, calling it "*a cause for profound concern.*"[1]

The two states are not allies as such, but the tension between the PRC and the West may push the two states even closer together. As pointed out by many before, the relationship between the PRC and Russia is based on pragmatism. Despite the supposedly personal relationship between Putin and Xi, there are areas of conflicting interests and a fundamental distrust

1 NATO, "Washington Summit Declaration 2024," Washington D.C., July 2024, https://www.nato.int/cps/en/natohq/official_texts_227678.htm.

between the two state actors.[2] This applies, for example, to the influence in Central Asia, which Russia sees as its legitimate post-Soviet sphere of interest. However, the war in Ukraine has weakened Russia's influence in the area, and the PRC has exploited this weakened position in order to optimize its own.[3] The PRC is even interfering in the core of the Slavic Brotherhood Alliance between Russia and Serbia, as the PRC consistently strengthens its cooperation with Belgrade.[4] The two-state actors are also competitors in the struggle for influence on the African continent, where they compete by different means: while Russia primarily offers PMCs for counter-terrorism, training and advice, the PRC facilitates cash and infrastructure projects.

Russia's war in Ukraine has given the PRC a possibility of increased access to the Arctic, even though it conflicts with Russia's attempt to minimize the influence of non-Arctic states in Arctic questions.[5] The self-declaration of the PRC as a 'near-Arctic state' seems to have worked.[6] Russia and the PRC share an interest in access to natural resources in the Arctic and have cooperated in infrastructure projects in the region.[7] Their individual interests, however, also potentially leave room for conflict of interests.

Since Russia's illegal invasion of Ukraine, the PRC has supported Russia's war—and Russia's ability to conduct the war, including informationally: the PRC has copied the Kremlin's euphemistic labeling of the full-scale invasion as a

2 Richard Q. Turcsányi, Jan Daniel, and Vojtěch Bahenský, "Dragon's Roar and Bear's Howl: Convergence in Sino-Russian Information Operations in NATO Countries?" (Latvia: NATO Strategic Communications Centre of Excellence, 2023), 14.

3 Danish Defence Intelligence Service, "INTELLIGENCE OUTLOOK 2023," 15.

4 Ljudmila Cvetkovic and Andy Heil, "What Is Behind Serbia and China's "Ironclad Friendship"?" *Radio Free Europe/Radio Liberty*, 14:18:42Z, sec. Serbia, https://www.rferl.org/a/serbia-xi-visit-china-relations-vucic-russia/32936674.html.

5 Danish Defence Intelligence Service, "INTELLIGENCE OUTLOOK 2023," 15.

6 David Merkle, "The Self-Proclaimed Near-Arctic State," International Reports, April 2023, https://www.kas.de/en/web/auslandsinformationen/artikel/detail/-/content/der-selbsternannte-fast-arktisstaat.

7 Jon Rahbek-Clemmensen and Camilla Tenna Nørup Sørensen (eds), *Sikkerhedspolitik i Arktis Og Nordatlanten*, 1. udgave, 2. oplag, Studier i Global Politik Og Sikkerhed 15 (København K: Djøf Forlag, 2021), 74.

'special military operation' and echoed Russian conspiracy theories about U.S. biological laboratories in Ukraine.[8] In the NATO Summit Declaration, the PRC is described as *'a decisive enabler'* for Russia's war and calls for the PRC to stop all political and material support to Russia's war effort.[9] Nevertheless, the NATO declaration has not deterred the PRC from continuing support to Russia. However, the "no limits" partnership has limits, which seem to coincide with the red line of possible sanctions and restrictions from the U.S. and the EU.

Ukraine is also an example of division between the two state actors when examining territorial claims, as the PRC has not recognized Crimea as Russian territory.[10] Also, Russia finds no support from the PRC when using its nuclear threat rhetoric.[11] Overall, it is fair to state that the relationship between the PRC and Russia is no marriage of love. However, a marriage of convenience is still a marriage, though the individual interests probably weigh in higher. That consequently also makes them more easily exploitable.

Different, but Comparable Approaches to Information Warfare

Russia's collective information apparatus is known for its multifaceted construct. On the contrary, the PRC's way of engaging in information warfare has been regarded as more simplistic and less sophisticated. Interestingly enough, despite the fact that the PLA has shown an explicit interest in information warfare since the 1990s, as described by Timothy Thomas back in 2004.[12] The

8 Mark Cozad, Cortez A. Cooper III, Alexis A. Blanc, David Woodworth, Anthony Atler, Kotryna Jukneviciute, Mark Hvizda, and Sale Lilly, "Future Scenarios for Sino-Russian Military Cooperation: Possibilities, Limitations, and Consequences," (Santa Monica, CA: Rand Corporation, 2024), 65, https://www.rand.org/pubs/research_reports/RRA2061-5.html.

9 NATO, "Washington Summit Declaration 2024," https://www.nato.int/cps/en/natohq/official_texts_227678.htm.

10 Mark Cozad, Cortez A. Cooper III, Alexis A. Blanc, David Woodworth, Anthony Atler, Kotryna Jukneviciute, Mark Hvizda, and Sale Lilly, "Future Scenarios for Sino-Russian Military Cooperation: Possibilities, Limitations, and Consequences," (Santa Monica, CA: RAND Corporation, 2024), 65.

11 Richard Q. Turcsányi, Jan Daniel, and Vojtěch Bahenský, "Dragon's Roar and Bear's Howl: Convergence in Sino-Russian Information Operations in NATO Countries?" (Latvia: NATO Strategic Communications Centre of Excellence, 2023), 5.

12 Timothy L. Thomas, "Like Adding Wings to the Tiger: Chinese Information War Theory and

concept of information warfare is also heavily examined in Qiao Liang and Wang Xiangsui's famous book 'Unrestricted Warfare' from 1999.[13]

Traditionally, the PRC's influencing activities in the West have mostly been thought of as either soft power initiatives, hard sticks or financial benefits: 1) Soft power initiatives such as the well-known 'Panda Diplomacy', Chinese New Year's celebration in cities outside China, and cultural-educational initiatives like Confucius Institutes at educational institutions. 2) The hard stick approach is the harsh response to any expressed or anticipated anti-PRC sentiment through official communication channels or through a digital army of PRC officials known as so-called Wolf Warriors attacking critics of the PRC online.[14] 3) Financial and infrastructural projects, with the Belt and Road Initiative as the most prominent one.[15]

The PRC, in contrast to Russia, still has the possibility of conducting some of its soft power initiatives. But, given the growing distrust between the PRC and the EU, a change has also been identified in its approach. The PRC has indeed learned from the Kremlin's playbook in regard to disinformation and has become more sophisticated in its approach. That includes target audience analysis and the Russian tradition of sowing doubt and using conspiracy theories[16]—including in the 2024 U.S. presidential election.[17]

Practice," (Foreign Military Studies Office, 2000).

13 Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing, PRC: PLA Literature and Arts Publishing House, 1999).

14 Duan Xiaolin and Liu Yitong, "The Rise and Fall of China's Wolf Warrior Diplomacy," *The Diplomat*, September 22, 2023, https://thediplomat.com/2023/09/the-rise-and-fall-of-chinas-wolf-warrior-diplomacy/ (accessed August 23, 2024).

15 Yu Jie and Jon Wallace, "What Is China's Belt and Road Initiative (BRI)?" Chatham House, updated December 19, 2022, https://www.chathamhouse.org/2021/09/what-chinas-belt-and-road-initiative-bri.

16 Richard Q. Turcsányi, Jan Daniel, and Vojtěch Bahenský, "Dragon's Roar and Bear's Howl: Convergence in Sino-Russian Information Operations in NATO Countries?" (Latvia: NATO Strategic Communications Centre of Excellence, 2023), 5.

17 Tiffany Hsu and Steven Lee Myers, "China's Advancing Efforts to Influence the U.S. Election Raise Alarms," *The New York Times*, April 1, 2024, https://www.nytimes.com/2024/04/01/business/media/china-online-disinformation-us-election.html.

Russia also seems to have learned from the PRC. Russia was the first to envision an isolated internet; however, while the concept of RuNet largely remained aspirational, the PRC expanded its 'Great Firewall' in a way Russia could only dream of.[18] During the pandemic, the PRC and Russia agreed on a common effort to combat disinformation. In the public statement from the PRC's Ministry of Foreign Affairs, it states that "*the two sides stressed that disinformation is a common enemy of the international community*" and that "*political viruses such as rumors and slanders and the perpetrators and manipulators behind the scene will have no place to hide.*"[19] The wording could indicate what we have since witnessed—an increasing focus on monitoring and acting on online behavior as well as restricting access to foreign services and trying to promote national alternatives.

In its Soviet past, Russia has been familiar with strict censorship and a strict repression apparatus, but recently it has learned some modern lessons from the PRC, especially in regard to establishing a new digital Iron Curtain dividing its own population from the West and the Western information environment. Prior to the Russian invasion of Ukraine in 2022, Western platforms such as Facebook, Instagram, and X (formerly Twitter) were still allowed in Russia—in contrast to the PRC. While Facebook, Instagram, and X were blocked quickly after the Russian invasion, other Western platforms stayed accessible. That includes YouTube and encrypted services such as Signal. In the summer of 2024, however, these services have also been subjected to restrictions.[20]

The two-state actors have both common and divergent interests, but both parties have an interest in maximizing mutual strategic objectives. Russia and

18 Daryna Antoniuk, "Russia Wants to Isolate Its Internet, but Experts Warn It Won't Be Easy," The Record, October 17, 2023, https://therecord.media/russia-internet-isolation-challenges (accessed August 25, 2024).

19 "Chinese and Russian Foreign Ministry Spokespersons Held Consultations and Agreed to Cooperate in Combating Disinformation," Ministry of Foreign Affairs of the People's Republic of China, July 25, 2020, https://www.mfa.gov.cn/eng/wjb/zzjg_663340/dozys_664276/xwlb_664278/202406/t20240606_11397578.html (accessed August 23, 2024).

20 "Russia Begins Blocking the Messenger Signal," Meduza, August 9, 2024, https://meduza.io/en/news/2024/08/09/russia-begins-blocking-the-messenger-signal (accessed August 23, 2024).

the PRC share the strategic objective of discrediting the U.S. and challenging its hegemonic status.[21] However, the strategy to achieving it differs from one another: Where Russia's strategy is disruptive, it is considered much more important for the PRC to promote a positive image of the country.[22]

Russia has partially compensated for the loss of its former European oil market by expanding exports to PRC and has extended an invitation to the PRC to the Artic table. The PRC can support Russia's war in Ukraine, among other things through proxies in order to avoid retaliation from the EU. In the information sphere, the PRC has been amplifying Russian rhetoric and narratives and supporting Russian viewpoints, when beneficial. The PRC's approval or at least acceptance of Russia's actions in Ukraine goes beyond the Chinese border; it is also paving the way to acceptance or understanding in other countries such as India and South Africa.[23] In return, the PRC cannot exploit Russia diplomatically in the West, but Russia's permanent seat in the UN Security Council can be useful for the PRC. Likewise, Russia can provide the PRC with an understanding of and access to a European information environment, including the use of Russia's digital infrastructure.[24] Both parties understand that this is transactional.

Framework for a Possible PRC-Russia Nordic Cooperation

China is, similarly to Russia, trying to weaken the European partnership with the United States. The PRC is increasingly using influence campaigns in order to promote the Chinese Communist Party's narrative about the PRC.

21 Richard Q. Turcsányi, Jan Daniel, and Vojtěch Bahenský, "Dragon's Roar and Bear's Howl: Convergence in Sino-Russian Information Operations in NATO Countries?" (Latvia: NATO Strategic Communications Centre of Excellence, 2023), 35.

22 Ibid.

23 Yu Jie, "China's Alignment with Putin Is Uneasy. But Its Rivalry with the US Makes Him Too Useful to Abandon," Chatham House, May 17, 2024, https://www.chathamhouse.org/2024/05/chinas-alignment-putin-uneasy-its-rivalry-us-makes-him-too-useful-abandon.

24 Richard Q. Turcsányi, Jan Daniel, and Vojtěch Bahenský, "Dragon's Roar and Bear's Howl: Convergence in Sino-Russian Information Operations in NATO Countries?" (Latvia: NATO Strategic Communications Centre of Excellence, 2023), 35.

This includes attempts to stifle criticism on sensitive issues, push European politics towards a more China-friendly direction, and sow discord to prevent a united, anti-China EU stance.[25] Acknowledging the fact that in 2023 and 2024, Norway,[26] Sweden,[27]Finland[28] and Denmark[29] have all signed a bilateral Defense Cooperation Agreement (DCS) with the U.S., sowing division and discord could easily become a theme of common interest.

The PRC has better diplomatic access to the Nordic countries, and Russia could try using Chinese voices and platforms as proxies for its own pro-Kremlin messaging. It could be done through a shared operation, if the PRC sees benefits in doing so. Having paved the way for the PRC to the Arctic table, Russia could try to exploit this for its own interest. If the PRC and Russia are able to find common ground on Arctic issues, it could strengthen each of their positions. If not, it could be a base for future conflicts.

Russia and the PRC do amplify each other's messaging on global television platforms like RT (formerly known as Russia Today) and CGTN (formerly known as CCTV), but it seems less likely that they will conduct social media campaigns on behalf of the other party. It seems more likely that social media campaigns of common interest will relate to anti-messaging, like anti-U.S. or anti-EU. These kinds of covert campaigns can use trolls, bots, or fake

25 Danish Defence Intelligence Service & Danish Security and Intelligence Service, "Vurdering Af Truslen Fra Fremmede Staters Påvirkningsvirksomhed i Forbindelse Med Europa-Parlamentsvalget Den 9. Juni 2024 [Assessment of the Threat from Foreign State Influence Activities in Connection with the European Parliament Elections on June 9, 2024]," May 2024.

26 Forsvarsdepartementet, "Norway and USA Agree on Additional Agreed Facilities and Areas under the SDCA," Nyhet, Regjeringen.no (regjeringen.no, February 2024), https://www.regjeringen.no/en/aktuelt/norway-and-usa-agree-on-additional-agreed-facilities-and-areas-under-the-sdca/id3023830/.

27 Government Offices of Sweden, "Defence Cooperation Agreement with the US Signed," Press Release, Ministry of Defence, December 6, 2023, https://www.government.se/press-releases/2023/12/defence-cooperation-agreement-with-the-us-signed/.

28 "Defence Cooperation Agreement with the United States (DCA)," Ministry for Foreign Affairs, https://um.fi/defence-cooperation-agreement-with-the-united-states-dca- (accessed August 24, 2024).

29 "New Agreement Strengthens Defence Cooperation between Denmark and the United States," Ministry of Defence, https://www.fmn.dk/en/news/2023/new-agreement-strengthens-defense-cooperation-between-denmark-and-the-united-states/ (accessed August 23, 2024).

and alternatively forged websites in order to spread disinformation including conspiracy theories.

The PRC's harsh approach to voices critical of the PRC might be efficient elsewhere, but in the Nordic countries, where the power distance between the authorities and the population is low, and people are used to expressing themselves as they want, it will more likely be counterproductive. The PRC's greatest tools of influence in the Nordic region seem to be more toward soft power and economy. That is at least in the short term, as the PRC's cooperation with and support of Russia's war in Ukraine could challenge that opportunity.

A cooperation could, of course, take many different forms: from learning from each other to joint campaigns. Based on the above, this chapter offers a simple framework for envisioning a possible enhanced PRC-Russia disinformation cooperation in the Nordic region:

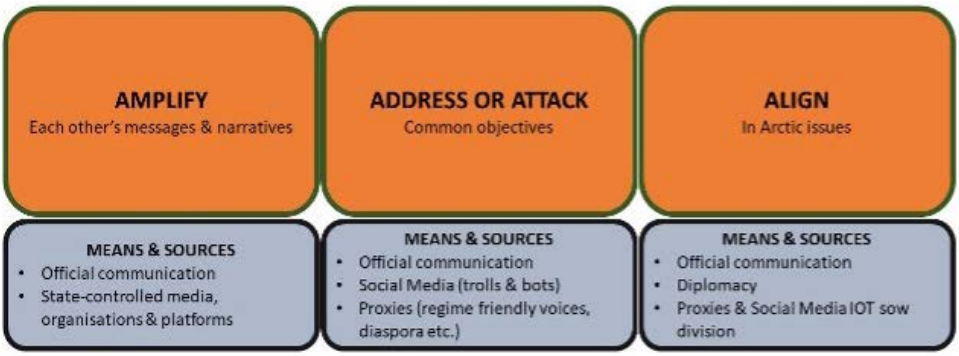

Illustration 1: A possible framework for an enhanced PRC-Russia disinformation cooperation.

The framework is by no means exhaustive but it provides a conceptual understanding of how and why messages and narratives are pushed to shape perception. The framework is not dependent on themes.

Nordic Response: A Framework for Protection & Mitigation

Threat perception may differ amongst the Nordic countries due to geography, history, and strategic culture. But many factors unite them. With Sweden and Finland in NATO, the path to closer Nordic military cooperation is more feasible. Furthermore, all countries have signed a Defence Cooperation Agreement with the U.S. All these countries are united in their support to Ukraine. Also, they are all democratic societies with freedom of press and expression: together with the Netherlands, these countries constitute the Top 5 in the Reporters Without Borders' Press Freedom Index.[30] Looking at risks, it indicates a Nordic information environment which is easily penetrable by malign interference. This is, however, also the outcome of generally well-educated societies with media literacy as a part of the educational system. But now we need more than that. We need disinformation-literacy: knowledge of the objectives behind disinformation, the ability to detect it, and awareness of its many forms and means; information laundering, forged media pages, use of proxies, etc., is important as a modern media consumer.

Initiatives such as the European Centre of Excellence for Countering Hybrid Threats[31] in Finland and the Psychological Defense Agency in Sweden assist in gathering knowledge and generating public awareness. So do the national intelligence assessments, public statements from authorities, and reports from fact-checking media. When identifying disinformation campaigns or malign interference, each nation should have a procedure in place for how to pre- and debunk foreign disinformation in its national information environment. In all these efforts, best practices should be shared within the Nordic countries.

When possible, identified disinformation campaigns should be publicly exposed and attributed. The chapter proposes another generic framework for such a Nordic response:

30 Reporters Without Borders, "Press Freedom Index 2024," 2024, https://rsf.org/en/index.

31 Hybrid CoE - The European Centre of Excellence for Countering Hybrid Threats, https://www.hybridcoe.fi/.

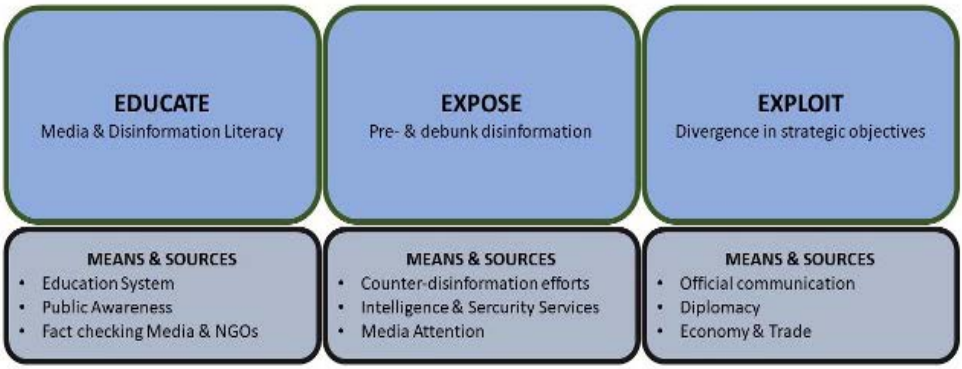

Illustration 2: A proposal for a framework for Nordic Response.

Even though there can be differences in the approach of Russia and the PRC to the Nordic countries individually, the overall themes of messaging are most likely to be alike. A collective Nordic response would also make the regional cognitive shield stronger, including establishing a better mutual understanding of the informational picture across the region.

Most importantly, it is possible that the PRC's appetite for amplifying pro-Kremlin and anti-Ukrainian messaging in the Nordic countries could be lowered by economic means. Perhaps not among the Nordic countries alone, but at least within the EU. Right now, the PRC's support of the Russian war does not cost the PRC anything.

It should be stressed that common objectives and common use of means do not necessarily equal a mutual interest: both the PRC and Russia conduct cyber operations, espionage and other destabilizing acts, including disinformation, independently. Likewise, activities conducted simultaneously do not necessarily equal a formalized cooperation. It can, though, still be a challenge for the Nordic region to handle if these two state actors initiate like-minded campaigns to shape perceptions.

Efficient countering of disinformation not only demands awareness and resources, but also political will to expose and exploit—and to punish malign behavior. The potential of exploiting the divergence of interest between the

PRC and Russia are low-hanging fruits. So is raising the cost for the PRC's war-support through economic instruments. A collective Nordic response would empower this effort.

To paraphrase Clausewitz, disinformation is a mere continuation of war by other means. Likewise, disinformation can be combatted by means other than communication.

7. Why "Mental Decoupling" is a Necessity for Ending Disinformation—and Could be the Start of a New Era for Business

Anna Rennéus Guthrie

"Information has never been as important as it is today."
"We (the West) have been naive."

These two statements are some of the most recurring shared truths the (geo) political debate feeds us repeatedly nowadays.

Both statements are arguably true, at least to some extent. However, if both of them are somewhat true and at the same time, it is quite shocking the way in which we go about our everyday affairs regarding information and security.

Before we dive further into what is being suggested, namely that we are living in times when we do not care about information in the way we ought to, given how the world is shaped, let us have a closer look at the larger context of security and the "securitization" of democratic societies that is developing.

Changing Superpowers, Changing World

There has been an uprising of security awareness on all levels of society in recent years. Naturally, one could have guessed that a war in Europe, like Russia's war on Ukraine, would lead to this. And so, it has. Yet, the years before the invasion in 2022 were already more security-oriented. This did not alone have to do with Putin's geopolitical ambitions, surfacing as they did in 2014 with Crimea and before that, in 2008 in Georgia.

In Sweden, where this text is produced, there has been in more recent years a general growing understanding that the happy days of the late 1990s and early 2000s, when globalization was a buzz- and not a curse word, are coming to an end. The change in our outlook derives not only as a reaction to the most obvious growing eastern threat but also from changes in our relationship with another superpower, China.

China has throughout the later decades of the 20th century experienced economic and innovative growth and under its current leadership distinctively heightened its ambitions on the global scene. There are numerous grand masterplans, five-year plans, and agendas for different prioritized industries and areas all aiming at world dominance: Made in China, China 2030, China Standards 2035, China 2050, the Belt and Road Initiative, and Health Silk Road, to mention a few. Running at the forefront of the development of cutting edge technologies such as AI and at the same time having access to the larger research community in the West has given China an upper hand.[1]

The strategic thinking and approach of a non-democratic country, where the political, business and military direction are aligned and basically one and the same, leads to an unfair playing field.

And the ambitions of the superpower do not stop at any given physical border. China has in the last years been called out by the Swedish Security Service as one of the greatest threats to Sweden.[2]

Visible marks of this new security situation were already seen in 2015, when Swedish citizen Gui Minhai was captured and imprisoned. And a few years

1 Paul Triolo and Kendra Schaefer, "China's Generative AI Ecosystem in 2024 Rising Investment and Expectations," The National Bureau of Asian Research, June 27, 2024, https://www.nbr.org/publication/chinas-generative-ai-ecosystem-in-2024-rising-investment-and-expectations/.

2 Swedish Security Service, "The Swedish Security Service 2023 – 2024," 2024, 28-29, https://sakerhetspolisen.se/ovriga-sidor/other-languages/english-engelska/press-room/swedish-security-services-annual-assesments.html; Rebecca Arcesati, "Europe Must Beef Up China Intelligence – Or Accept US Bullying," Center for European Policy Analysis, May 10, 2024, https://cepa.org/article/europe-must-beef-up-china-intelligence-or-accept-us-bullying/.

on, a somewhat aggressive Chinese ambassador to Sweden who tried to silence Swedish journalists, and numerous attempts made by unknown subjects to alter and shut down seminars and talks on "sensitive issues" for China in Sweden. The rocky road with China has continued since then.

In fact, the proximity to authoritarian states that globalization has offered us through intensified trade, travel, research and cultural exchange has through events such as these become more strenuous to carry off for every incident and scandal that left "us", on the democratic side, with less when the full calculation was done. Having a full stomach and going to bed in your own house suddenly did not feel as great as it once used to. Even if the ceiling still is there, the insecurity of not knowing who to trust and that the world is undergoing more negative changes became increasingly evident to a lot more people during the last decade.

The War On Us

With the Russians' full scale invasion of Ukraine on February 24, 2022, there was a sense of urgency practically overnight that Europe was facing a new harsh reality. Today, most Europeans and their leaders realize and fear the threat as their own. This has led to an increase in defense spending and planning as well as a range of new policies, recommendations and even legislation to tackle the new unsecure times.

When the term securitization is used about the changes in how society handles outbursts of crises, terror or war, this is quite often with either the direct or implied association of something unnecessary or exaggerated. However, as the war in Ukraine continues, and the evil intentions of additional aggressors and war makers surface, so does the impulse to remain passive towards real threats weaken.

The story we have been telling ourselves during recent decades, mainly for good reasons, and still actually in part tell, is that through meeting and engaging with others, through business and research, competition and economy, our potential to grow and even our way of living will grow and

expand for the better for everyone. This narrative is such an attractive one that it is not worth questioning—even in the worst patches of turmoil which war and terror brings.

Of course, arguably *freedoms of all forms such as thought, action, markets and enterprises will in the long run be the solution to oppression and domination*—but only consistently and in depth when conducted under a veil of integrity and comradeship with equal or semi-equal partners, and that in a context where to strive for the great good is the similar, and essentially, *greater* good.

Parallel to this developing heightened awareness of security risks and staunch support for Ukraine, the integration of Chinese owned technology in the West has continued to cause disturbances without proper preemptive measures being implemented.

More Meeting Places - Less Meeting

We have, in fact, not yet properly addressed the problematic relationship when it comes to the sphere of information technology, media and communications. The connectivity characteristics of these technologies make them *the essential meeting ground* where the test of exchange is truly put to the test, so to speak.

In previous generations, changing a national narrative took time, effort and language skills. These obstacles made it more difficult to penetrate larger groups with malign foreign narratives, as well as more positive forms of reaching out to the other.

Looking at the topics and sensitive issues that are prioritized by European governments and agencies, the focus heavily lies on critical assets and infrastructure in its physical meaning. It also lies on threats deriving from cybercrime and espionage, rather than influence operations. The Swedish ban on Huawei in 2022 is an example of this.[3] The Swedish authorities, just as their

3 Kelvin Chan, "Sweden bans Huawei, ZTE from 5G, calls China biggest threat," *Associated Press*, October 20, 2020, https://apnews.com/article/sweden-china-europe-telecommunications-security-services-586826c6aa02d1571c8b4d6840043931.

American counterparts, and a number of other European countries, as well as Japan, Taiwan and Australia, identified safety risks with Chinese telecom companies entering 5G core networks.[4] However, the psychological warfare and its toolbox with China as the perpetrator is still more of a conundrum for politics to solve, while the main focus is Russia.

Even if there has been a bit of a fight, primarily from the American side, about Chinese ByteDance-related TikTok, the world-renowned communication platform that attracts the young and the uneducated, its presence and stance is still strong and growing in the West.[5]

TikTok is undoubtedly a very sharp tool in a potential toolbox the day it is seized and made full use of directly by the Chinese government. In the beginning, suspicions about data leakage and risk of using the entertainment channel for surveillance were brushed off as "protectionism" and at times even called a U.S. strategy for diminishing China as a tech rival. During more recent years and months, more qualified studies about another threat, potentially of equal or even larger importance, have materialized. Studies and research on the content and the working of TikTok algorithms have made the picture evidently clear.[6] There is less room for topics and narratives that challenge the Chinese state on the app produced by an offspring of a Chinese state-owned enterprise.

---

4 Alina Clasen, "EU Commission bans Huawei, ZTE, urges countries to do the same," Euractive, Jube 16, 2023, https://www.euractiv.com/section/cybersecurity/news/eu-commission-bans-huwai-zte-urges-countries-to-do-the-same/.

5 Pieter Haeck, "Europe is nowhere close to banning TikTok," *Politico*, May 3, 2024, https://www.politico.eu/article/us-style-tiktok-ban-nowhere-close-europe/; Lisa O'Carroll, "TikTok questioned by EU over Lite app that 'pays' users for watching videos," *The Guardian*, April 17, 2024, https://www.theguardian.com/technology/2024/apr/17/tiktok-questioned-lite-app-eu-children-addiction.

6 Alex Goldenberg, et al., "The CCP's Digital Charm Offensive: How TikTok's Search Algorithm and Pro-China Influence Networks Indoctrinate GenZ Users in the United States," Network Contagion Research Institute Intelligence Report 2024, https://networkcontagion.us/wp-content/uploads/NCRI-Report_-The-CCPs-Digital-Charm-Offensive.pdf; Anna Rennéus Guthrie and Patrik Oksanen, "Tiktok: barnunderhållningen som blev ett säkerhetsproblem [Tiktok: the children's entertainment that turned a security issue]," Stockholm Free World Forum Report No. 2023:2, https://frivarld.se/wp-content/uploads/2023/03/TikTok.pdf.

Being the primary news provider[7] to a large group of the world's population comes with responsibilities. However, we should not fool ourselves into believing that this responsibility is interpreted similarly to how companies formed in a democratic society interpret their business model.[8]

Companies originating from China have an obligation to report back to their national security agencies and it is the world's most undisclosed secret that every Chinese citizen is obliged to report home issues of relevance to the state of China, when asked to do so, or even more preferred, voluntarily. As the Chinese state has golden shares in TikTok's parent company ByteDance, the state's presence is arguably even more direct.

The backsliding of freedom in Hong Kong during the last few years and the new security laws which China has enforced upon the former free marketplace is an illustration and sharp warning of how China views individual freedom nowadays, not only at home but outside of Mainland China. So is the continued escalation of aggression demonstrated towards Taiwan,[9] as well as the more recent approaches in Japanese airspace.[10]

NATO concluded just recently, but importantly, that China is now no longer to be regarded as a strategic competitor but rather an aggressor, or as the

---

7 Katerina Eva Matsa, "More Americans are getting news on TikTok, bucking the trend seen on most other social media sites," Pew Research Center, November 15, 2023, https://www.pewresearch.org/short-reads/2023/11/15/more-americans-are-getting-news-on-tiktok-bucking-the-trend-seen-on-most-other-social-media-sites/?utm_content=buffer6434a&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer-pew.

8 Alicja Bachulska, "Behind the buzzwords: What China's priorities mean for Europe," European Council on Foreign Relations, August 9, 2023, https://ecfr.eu/article/behind-the-buzzwords-what-chinas-priorities-mean-for-europe/.

9 Matthew Sperzel and Daniel Shats, "China-Taiwan Weekly Update: August 30, 2024," Institute for the Study of War, August 30, 2024, https://www.understandingwar.org/backgrounder/china-taiwan-weekly-update-august-30-2024.

10 Takahashi Kosuke, "Japan Confirms First-Ever Airspace Intrusion by a Chinese Military Aircraft," *The Diplomat*, August 27, 2024, https://thediplomat.com/2024/08/japan-confirms-first-ever-airspace-intrusion-by-a-chinese-military-aircraft/#:~:text=A%20Chinese%20military%20Y%2D9%20intelligence%2Dgathering%20aircraft%20was%20spotted,a.m.%20on%20the%20same%20day.

wording was, a "decisive enabler" in Russia's war in Ukraine, a war Russia has started in Europe.[11]

This wording is not merely of relevance for a military or security community.[12] The shift affects all of us. From ordinary citizens to international companies. It is, therefore, crucial to address the threat with a whole of-society—or rather societies—approach. Tackling the threat at the moment, as we are doing, in separate confined boxes, where the private, public and academic sectors lack a continuous and honest dialogue about these threats, is far from efficient. Even if small steps in the right direction are better than doing nothing.

When it comes to disinformation, we have come to learn that China mainly piggybacks on Russia's campaigns, in which narratives around NATO are central. Not fully mastering the techniques, or cultural context, which makes disinformation take root in a western context, there are still numerous pro-China narratives which we have grown used to that maintain the idea that China is so big and mighty that the West cannot handle its future without a deep codependency.

These narratives do not, in fact, necessarily need to stem from China. As they carry so much of our own vulnerabilities in them, they tend to make sense from our own way of thinking about ourselves.

Some of these particular narratives are:
We cannot solve climate change without China.
We cannot innovate without China.
Without China, the war in Ukraine would be even worse.

11 North Atlantic Treaty Organization, "Washington Summit Declaration," July 10, 2024, https://www.nato.int/cps/en/natohq/official_texts_227678.htm.

12 Anna Rennéus Guthrie, "Temperaturmätare – så ser svenska företag och lärosäten på utbyten med Kina [Temperature Gauge – How Swedish Companies and Academic Institutions View Exchanges with China]," Stockholm Free World Forum, October 2021, https://frivarld.se/wp-content/uploads/2021/12/Kina-Rapport-.pdf.

All of these statements are in various shapes regularly flaunted in the media, in the political debate, and within relevant communities be it the political, business or media sphere.

All of the above could, of course, be arguable in parts. But the pattern in them is that they cast China as the stronger part. The message is consistently that the strength is with China not the West, and this is of course deteriorating in the long run.

Call for Protective Mental Walls

To protect the foundation of our society and build our psychological defense structures, we need to start building our own mental wall. Just as we have called out Russian disinformation and Putin's "negotiations" as false at its core, we need to learn that even if the Chinese state is not a manipulator in the Russian sense, there is a constant unreliability and aggression which has a clear ambition to undermine the foundations of western society in a whole of society, whole of nations, and whole of continent approach.

Repeating the mantra that "we have been naive" will not be helpful. In fact, it needs to be replaced directly with something more assertive and signaling inward that a new era has begun. "We know better now" would, for instance, be a good start demonstrating that we will not be satisfied with being overrun again.

Living in an information society, we are definitely not paying enough attention to the impact of information nor acting upon the information that is accessible. *Mentally withdrawing from the enabler of war is in fact the only way of protecting the core of our free world* and our societies, as well as quite importantly, hindering the next generation from growing up assuming that there is no difference between free and authoritarian societies, that all information is neutral and/or that the liberal word order demands a balancing act offered by states of other ideological origins.

We need to get used to the thought that de-coupling as such, in a broad and general sense, lies not in our arms anymore. We cannot bear the

responsibility of possibly losing to China, as we are not the aggressor or active subject here.

From Challenge to Business Opportunity?

Instead, by using our own power in decision-making, we can constructively steer away from further involvement with harmful propaganda. Using Chinese-owned communications systems, whether it is for public surveillance, news information or political debate, is likely not the best option for the police, the teenage boy or the parliamentarian of a free society. Rather the opposite.

In fact, we ought to treat the "challenges" as possibilities, learning from other domains. The last few decades have largely centered on environmental issues and the climate challenge in the West. In the beginning, few businesses thought that focusing on cutting down on carbon and adapting to new sources of energy would be helpful. Today, it is part of many of the largest companies' business models.

Handled properly, what today faces us living in the free world is a challenge of enormous proportions, and it could even become the beginning of a new era. An era where security is not an add-on, an extra layer, but rather a necessity for doing business within both the closest group as with the larger world.

The first place to start this would naturally be within the realms of information and media.

While the business and economy sectors try to grapple with the essentials of derisking and thus adjusting what has been a very naive—and/or comfortable position—towards China, let us properly pull the plug regarding information leakage and vulnerable news and media platforms.

If we are hindered in this regard by legislation and golden rules of our own value systems, such as free market and enterprise, let us instead assertively use our freedom of choice and speech, and make it very clear for any one in doubt, that "a penny for your thought"—which is what TikTok's business

model also offers whilst trying to attract new users to sign-up—is a very poor choice for the salesman, an ordinary and often juvenile, human being, in this context.

The underlying conflict we are experiencing in regard to China, just as we will be with any aggressor of economic and political relevance, is fueled by contesting goals such as "freedom of research" and "free trade", which are set against safeguarding the democratic free society in its foundations. This is the knot we need to unravel.

Embracing communications platforms tied to a communist state and the narratives that support them will not bring more freedom or prosperity to the world. Neither will selling out the essence of what made us prosperous to start with. The earlier we admit this, the easier it will be to find a more secure path from where we are now.

8. Peace-Keeping Role of Independent Fact-Checking in Polarized Democracies: A Case Study of the Taiwan FactCheck Center during the 2024 Presidential Election

Shih-Hung Lo

Disinformation poses a significant threat to democratic processes worldwide, particularly during elections when misleading narratives can manipulate public opinion, deepen societal divisions, and undermine electoral integrity. Taiwan's 2024 Presidential Election serves as a stark example of these challenges, as the nation continues to be the most disinformation-targeted country globally, according to the Varieties of Democracy (V-Dem) report. Disinformation campaigns, primarily orchestrated by China, exploit Taiwan's vibrant digital democracy, seeking to destabilize its political system. In this volatile context, the Taiwan FactCheck Center (TFC) has emerged as a critical peace-keeping force, countering disinformation, safeguarding public trust, and ensuring the integrity of the electoral process.

This chapter explores TFC's strategic responses to disinformation during the 2024 presidential election, highlighting its essential role in maintaining democratic stability and the broader implications for democracies worldwide.

Taiwan: A Prime Target of Disinformation

For the 11th consecutive year, Taiwan was ranked as the country most affected by disinformation, primarily due to aggressive campaigns originating from China. According to the 2024 V-Dem report, Taiwan's disinformation score of 0.092 was the lowest among the countries surveyed, indicating a high level

of impact compared to other heavily targeted nations.[1]. These campaigns are strategically designed to undermine Taiwan's democratic institutions, question its sovereignty, and weaken public confidence in the government's ability to protect its citizens.

China's disinformation tactics include leveraging Hong Kong as a hub for disseminating propaganda, which provides a veneer of separation between Chinese state actors and the information operations conducted against Taiwan. The spread of disinformation aims to erode international support for Taiwan, paint the island as unstable, and depict its government as incapable of defending against external threats. Such disinformation efforts are intended to make Taiwan appear vulnerable, potentially discouraging foreign nations from providing assistance in the event of a Chinese attack.[2]

Disinformation in the 2024 Presidential Election

The disinformation campaigns during the 2024 election were marked by several prominent themes. Among these were false narratives about alleged election fraud, attempts to delegitimize candidates, and fearmongering regarding Taiwan's national security, particularly concerning tensions in the Taiwan Strait.[3] These tactics are not new but have been refined over time, drawing on disinformation strategies that have proven effective in other geopolitical contexts. The research highlights how China's approach in Taiwan closely resembles Russia's disinformation tactics, particularly in how narratives are crafted to erode trust in democratic processes.[4]

---

1 M. Yang W. Hetherington, "Taiwan most affected by disinformation," *Taipei Times*, March 25, 2024, https://www.taipeitimes.com/News/taiwan/archives/2024/03/25/2003815440 (accessed September 7, 2024).

2 Ibid.

3 W. P. Li, "Inciting anxiety about the looming war -the disinformation narratives about the possible Taiwan Strait crisis during the 2024 Taiwanese presidential election," Taiwan FactCheck Center, November 27, 2023, https://tfc-taiwan.org.tw/articles/9931 (accessed September 7, 2024).

4 L. Győri, P. Krekó, and B. Zöldi, "China uses the Kremlin's cookbook when spreading disinformation in Taiwan," *Lakmusz*, January 18, 2023, https://www.lakmusz.hu/china-uses-the-kremlins-cookbook-when-spreading-disinformation-in-taiwan/ (accessed August 20, 2024).

At the same time, the 2024 Taiwan presidential election was also one of the most fiercely contested in recent history, marked by a flood of disinformation campaigns primarily orchestrated by Chinese actors aiming to manipulate public opinion and disrupt the electoral process. These campaigns employed sophisticated tactics, including deepfake videos, AI-generated content, and coordinated bot networks, which were designed to amplify false narratives and sow distrust among voters. In the weeks leading up to the election, rumors about vote fraud and electoral mismanagement began to circulate widely, creating a toxic atmosphere of suspicion and uncertainty. One of the most damaging disinformation pieces was a video showing an election worker mistakenly entering a vote in the wrong column, which was edited to appear as though it was part of a broader pattern of intentional voter fraud.[5]

The spread of this video on social media platforms such as TikTok, Facebook, and LINE had the potential to incite public outrage and undermine the legitimacy of the entire electoral process. The rapid and wide dissemination of such manipulated videos highlighted the challenges faced by fact-checkers like the Taiwan FactCheck Center (TFC) in countering misinformation in real time. TFC's swift response was critical in debunking the video, demonstrating that the alleged vote manipulation was a simple human error that was quickly corrected by election staff on-site. This timely clarification helped to prevent the disinformation from taking root and reassured the public that the electoral process remained secure and transparent.[6]

Beyond vote fraud, the 2024 election also saw a surge in disinformation targeting candidates directly, aiming to discredit their reputations and sway voter perceptions. For instance, false narratives were circulated about DPP

5 D. Klepper and H. Wu, "How Taiwan beat back disinformation and preserved the integrity of its election," *AP News*, January 27, 2024, https://apnews.com/article/taiwan-election-china-disinformation-vote-fraud-4968ef08fd13821e359b8e195b12919c (accessed August 25, 2024); W. P. Li, "Dissecting the false claims of electoral fraud in the 2024 Taiwanese presidential election," Taiwan FactCheck Center, February 5, 2024, https://tfc-taiwan.org.tw/articles/10284 (accessed August 21, 2024).

6 W. P. Li, "Dissecting the false claims of electoral fraud in the 2024 Taiwanese presidential election," Taiwan FactCheck Center, February 5, 2024.

candidate Lai Ching-te, accusing him of unethical behavior and spreading unverified rumors about his personal life. These attacks were not only meant to undermine Lai's credibility but also to create a broader sense of chaos and distrust among voters. Similarly, misleading claims about his running mate Hsiao Bi-khim, including assertions that she still held U.S. citizenship and was therefore ineligible for office, were debunked by TFC, which provided clear evidence refuting these falsehoods. By addressing these targeted disinformation campaigns, TFC played a vital role in preserving the integrity of the election and ensuring that voters were not misled by baseless claims.[7]

Additionally, narratives questioning Taiwan's international alliances, particularly its relationship with the United States, were prevalent in the disinformation landscape. These narratives sought to paint the DPP as reckless and inclined to provoke unnecessary conflict, thus swaying voters towards candidates perceived as more conciliatory towards China. By dissecting these claims and providing accurate context, TFC helped maintain a balanced public discourse, ensuring that misinformation did not unduly influence voter decisions. TFC's efforts to address the breadth of disinformation themes during the 2024 election underscored its essential role in safeguarding democratic processes against manipulation and foreign interference.

Role of Civic Technology in Combating Disinformation

Taiwan's approach to combating disinformation is distinguished by its innovative use of civic technology, which has empowered civil society organizations (CSOs) to play a vital role in preserving information integrity. CSOs like g0v and Cofacts have leveraged transparency, open-source collaboration, and civic engagement to counter disinformation effectively, creating a robust ecosystem of digital democracy. According to Irene Chou and Tatiana Van den Haute, the g0v movement epitomizes this approach, bringing together civic hackers, experts, and community members to enhance government transparency and public participation through digital tools.[8]

7 Ibid.

8 I. Chou and T. Van den Haute, "The evolving role of civic tech against disinformation in digital

The g0v community's ethos of open cooperation is exemplified by initiatives like vTaiwan, a decentralized open consultation process that combines online and offline interactions to facilitate crowdsourced lawmaking. vTaiwan has successfully engaged citizens, industry experts, and government representatives in policy discussions, enhancing the legitimacy of policymaking through broader consultation. Although vTaiwan's recommendations are not legally binding, the initiative has influenced significant regulatory changes, such as the regulation of online alcohol sales and Uber, showcasing the potential of civic tech to reshape democratic governance.[9]

Cofacts, another prominent g0v-inspired initiative, directly addresses the challenge of disinformation by using a crowdsourced fact-checking model. Launched in 2016, Cofacts operates a chatbot on LINE, Taiwan's most popular messaging app, allowing users to submit questionable information for verification. The platform's open participation model enables citizens to actively engage in fact-checking, fostering a culture of media literacy and public accountability. Cofacts' innovative approach to crowdsourcing fact-checks not only ensures a rapid response to disinformation but also builds public trust in the fact-checking process, reinforcing the democratic ideals of transparency and citizen involvement.[10]

Strategic Responses and Peace-Keeping Efforts by TFC

In response to the pervasive threat of disinformation, the Taiwan FactCheck Center (TFC) adopted a multifaceted strategy that integrates real-time fact-checking, public education, media collaboration, and engagement with civic tech communities. This comprehensive approach reflects TFC's commitment to transparency and impartiality, ensuring that its interventions are perceived as credible across Taiwan's politically diverse landscape. A key component of TFC's strategy is its rapid response mechanism, which involves continuous monitoring of information flows across social media and digital platforms.

democracy," *CommonWealth Magazine*, April 29, 2024, https://english.cw.com.tw/article/article.action?id=3678 (accessed August 28, 2024).

9 Ibid.

10 Ibid.

This enables TFC to swiftly identify and debunk false claims before they gain significant traction, thereby preventing misinformation from shaping public opinion.[11]

One of the most effective elements of TFC's strategy is its non-partisan stance, which has allowed it to earn the trust of political actors across the spectrum. During the 2024 election, TFC's fact-checks were frequently cited by candidates from all major parties, including the Democratic Progressive Party (DPP), the Taiwan People's Party (TPP), and the Kuomintang (KMT), as they sought to counter misinformation targeting their campaigns. This widespread reliance on TFC's findings underscored the center's role as a neutral arbiter of truth and highlighted its capacity to act as a stabilizing force in a highly polarized environment. TFC's impartial and rigorous approach to fact-checking created a common platform where verified information could transcend partisan divides, reinforcing the essential role of fact-based discourse in maintaining electoral integrity.[12]

Additionally, TFC actively collaborated with other civic tech initiatives such as Cofacts and the g0v community, utilizing their open-source, crowdsourced platforms to broaden the reach and impact of its fact-checking efforts. These partnerships allowed TFC to leverage a larger network of citizen fact-checkers, tech developers, and volunteers, enhancing its capacity to identify and verify misinformation rapidly. For instance, TFC's collaboration with Cofacts involved the use of automated tools, such as chatbots on LINE, to deliver instant fact-checking services to the public. This innovative approach not only expedited the debunking process but also empowered ordinary citizens to participate in combating disinformation, fostering a collective sense of responsibility toward maintaining information integrity.[13]

---

11 L. Győri, P. Krekó, and B. Zöldi, "China uses the Kremlin's cookbook when spreading disinformation in Taiwan," *Lakmusz*, January 18, 2023.

12 D. Klepper and H. Wu, "How Taiwan beat back disinformation and preserved the integrity of its election," *AP News*, January 27, 2024.

13 I. Chou and T. Van den Haute, "The evolving role of civic tech against disinformation in digital democracy," *CommonWealth Magazine*, April 29, 2024.

Moreover, TFC has emphasized public education and media literacy as fundamental aspects of its strategy. Through workshops, public campaigns, and online resources, TFC has sought to equip the public with the skills necessary to critically evaluate information and recognize disinformation tactics. This educational outreach aims to build a more informed and resilient electorate capable of discerning truth from falsehood, thereby contributing to the long-term stability of Taiwan's democratic framework. By empowering citizens with the knowledge to challenge disinformation, TFC not only addresses immediate threats but also strengthens the democratic fabric of Taiwan, showcasing how fact-checking can serve as a crucial defense against the destabilizing effects of misinformation in democratic societies.

Addressing Key Disinformation Themes

During the 2024 presidential election, the Taiwan FactCheck Center (TFC) played a crucial role in addressing key disinformation themes that threatened public trust and electoral stability. A prevalent narrative involved allegations of widespread vote fraud, propagated primarily through selectively edited videos that misrepresented the actions of election workers. These videos were strategically disseminated across social media platforms, aiming to amplify public distrust in the electoral process. TFC's prompt and systematic fact-checking of these false claims was instrumental in providing the public with accurate information, thereby mitigating the potential damage to the credibility of the election results.[14] By swiftly correcting false narratives, TFC effectively prevented these misleading claims from escalating into broader controversies that could have undermined the legitimacy of the electoral process.

TFC also focused on countering disinformation targeting Taiwan's international relations, particularly narratives that sought to erode public confidence in the reliability of U.S. support for Taiwan. Chinese disinformation efforts frequently portrayed the DPP as reckless and likely to provoke conflict with China, with the aim of influencing voters to favor pro-China candidates.

14 L. Győri, P. Krekó, and B. Zöldi, "China uses the Kremlin's cookbook when spreading disinformation in Taiwan," *Lakmusz*, January 18, 2023; D. Klepper and H. Wu, "How Taiwan beat back disinformation and preserved the integrity of its election," *AP News*, January 27, 2024.

These narratives exploited existing public anxieties regarding national security and Taiwan's diplomatic standing. Through rigorous, evidence-based rebuttals, TFC effectively countered these disinformation efforts, maintaining public trust in Taiwan's foreign policy decisions and thwarting external attempts to manipulate voter perceptions.[15]

Furthermore, TFC addressed disinformation aimed at discrediting individual candidates through personal attacks and fabricated scandals. Notable examples included false claims about the personal life of DPP candidate Lai Ching-te and unfounded rumors regarding the eligibility of his running mate, Hsiao Bi-khim. TFC's systematic investigations into these allegations ensured that voters could make informed decisions based on verified information rather than misleading rumors. This work not only safeguarded the reputations of the affected candidates but also reinforced the integrity of the democratic process, underscoring the critical importance of factual accuracy in electoral discourse. By confronting these targeted disinformation campaigns, TFC played a pivotal role in sustaining a credible and fair election environment, demonstrating its capacity to act as a vital defense against the disruptive forces of misinformation.

Challenges Faced by TFC and Civic Tech Initiatives

Despite the proactive measures taken by the Taiwan FactCheck Center, the organization encountered significant challenges during the 2024 election cycle, particularly in responding to the scale and sophistication of disinformation campaigns. Many of these campaigns involved coordinated, AI-driven strategies that employed fake accounts, manipulated media, and other advanced technologies to disseminate false narratives rapidly. The complexity and sheer volume of these disinformation operations presented a formidable challenge to real-time fact-checking efforts, making it increasingly difficult for TFC to detect and counteract misleading content in a timely manner.[16]

15 R. Iyengar, "How China exploited Taiwan's election—and what it could do next," *Foreign Policy*, January 23, 2024, https://foreignpolicy.com/2024/01/23/taiwan-election-china-disinformation-influence-interference/ (accessed August 17, 2024).

16 L. Győri, P. Krekó, and B. Zöldi, "China uses the Kremlin's cookbook when spreading disinformation in Taiwan," *Lakmusz*, January 18, 2023.

Civic tech initiatives like Cofacts also faced substantial obstacles in their efforts to combat disinformation, primarily due to their reliance on crowdsourced fact-checking models. While this approach allows for rapid engagement with disinformation, the dependence on volunteer contributions often limits scalability and operational efficiency, especially when contrasted with the extensive resources available to state-backed disinformation campaigns. The volunteer-driven nature of these initiatives frequently results in a mismatch between the scale of the disinformation problem and the capacity to address it effectively, highlighting a critical gap in the current fact-checking infrastructure.[17]

Maintaining neutrality and independence poses an additional challenge for TFC and similar fact-checking organizations operating in politically polarized environments. Perceptions of bias can significantly undermine public trust, necessitating rigorous standards of transparency and accountability throughout the fact-checking process. TFC's commitment to publishing detailed reports and methodologies has been instrumental in preserving its credibility; however, the organization must continually navigate the complex political dynamics of Taiwan to ensure impartiality and maintain public confidence.

Furthermore, the funding models of civic tech projects like Cofacts, which prioritize financial independence through crowdfunding and volunteer support, present ongoing sustainability challenges. Unlike some fact-checking organizations that receive funding from major tech companies such as Meta and Google, Cofacts emphasizes avoiding potential conflicts of interest through its independent financial structure. However, this approach requires constant efforts to secure sufficient resources and maintain an active volunteer base, underscoring the need for diversified funding strategies that can support the long-term effectiveness and resilience of civic tech initiatives in the fight against disinformation.

17 I. Chou and T. Van den Haute, "The evolving role of civic tech against disinformation in digital democracy," *CommonWealth Magazine*, April 29, 2024.

Broader Implications for Global Democracies

Taiwan's experience in combating disinformation offers valuable lessons for other democracies facing similar challenges. The island's innovative use of civic tech, coupled with a whole-of-society approach that engages government, civil society, and the private sector, provides a model for how democracies can effectively counter disinformation while preserving freedom of expression. As the world's most targeted nation for disinformation, Taiwan's resilience demonstrates the importance of cross-sector collaboration, transparency, and civic engagement in maintaining democratic stability.

The success of TFC and other CSOs in Taiwan also highlights the critical role of independent fact-checking as a safeguard against democratic erosion. As A.G. Sulzberger noted, the ability to question established narratives and provide nuanced, accurate information is essential to a healthy democracy.[18]. By fulfilling this role, TFC has helped protect Taiwan's democracy from the destabilizing effects of disinformation, serving as a beacon of resilience in the face of sophisticated information warfare.

Conclusion

The Taiwan FactCheck Center's efforts during the 2024 presidential election demonstrate the essential role of independent fact-checking in maintaining democratic stability, particularly in the face of sophisticated disinformation campaigns. As Taiwan continues to be a primary target of disinformation, primarily from China, TFC's work highlights the importance of a proactive, transparent, and collaborative approach to safeguarding electoral integrity. By countering false narratives swiftly and accurately, TFC not only protected the democratic process but also reinforced the public's trust in Taiwan's institutions at a critical moment in the nation's history.

Moreover, Taiwan's experience underscores the broader need for democracies worldwide to invest in independent fact-checking organizations, civic tech

18 A. G. Sulzberger, "Journalism's essential value," *Columbia Journalism Review*, May 15, 2023, https://www.cjr.org/special_report/ag-sulzberger-new-york-times-journalisms-essential-value-objectivity-independence.php (accessed August 20, 2024).

initiatives, and media literacy programs. The success of TFC, along with civic tech projects like Cofacts and g0v, provides a roadmap for how other countries can build resilient information ecosystems that defend against disinformation while promoting citizen engagement and transparency. This whole-of-society approach—where governments, civil society, and private citizens work in unison—offers a powerful defense against the growing tide of misinformation that threatens democratic governance globally.

As democracies continue to grapple with the challenges posed by foreign and domestic disinformation, Taiwan's model serves as both a cautionary tale and a source of inspiration. It illustrates the critical balance needed between regulation and freedom of expression, highlighting the importance of empowering citizens through transparency and civic participation. The lessons learned from Taiwan's ongoing battle against disinformation are not just relevant for its own survival but are vital for the preservation of democratic values worldwide. In an era where truth is constantly under siege, the commitment to fact-checking, open collaboration, and public education will remain fundamental to the health and resilience of democratic societies.

9. United Against Disinformation: Challenges and Recommendations for Addressing the Transnational Threat of Disinformation by Authoritarian States

Wei-Ping Li and Eve Chiu

The world has witnessed the power of disinformation in recent years, beginning with the 2016 U.S. presidential election, when the international community was taken aback by how false information interfered with elections, and continuing through significant events such as the COVID-19 pandemic, the Russia-Ukraine War, and the Israel-Gaza War. If frontline fact-checkers, journalists, and academics have learned anything from the fights against disinformation, it is that the threats posed by disinformation do not only impact one country. Instead, it is a serious problem that affects all societies that value democracy and the importance of truth. To effectively tackle disinformation, democratic countries should enhance cross-regional and cross-sectoral collaborations. In this chapter, we will discuss the challenges in combating disinformation and offer recommendations on what governments and policymakers may do to foster greater international cooperation.

An Example of How Pro-Kremlin Disinformation became a Chinese Propaganda Tool

In this chapter, we define disinformation as pieces of false information deliberately produced by malicious actors.[1] These actors can be authoritarian governments or agents for the governments, such as public relations

1 C. Wardle and H. Derakhshan, *Information disorder: Toward an interdisciplinary framework for research and policy making* (Council of Europe Publishing, 2017), https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html.

firms seeking profits or individuals who have specific purposes.[2] Once a disinformation piece is created, it may be shared, amplified, or modified by numerous propagators for various reasons, targeting audiences in different places and resulting in various outcomes. There are several opportunities for involved actors to exploit information throughout the disinformation creation, transmission, and audience reception processes. These actors may or may not coordinate. However, the false claims they produce can negatively impact many audiences across geographic regions. Over the past years, malicious actors have frequently taken this approach to wield influence whenever significant world events occur. One example is the disinformation campaign waged during the Russia-Ukraine War, which promoted false messages that NATO was at war with Russia in Ukraine and had encountered setbacks.

Among this strain of false claims, one spread in early April 2022 asserted that the Russian army had captured U.S. Major General Roger L. Cloutier Jr. in the besieged Ukrainian Azov camp in Mariupol. According to PolitiFact's fact-checking, this message surfaced on X and was then promoted by fringe online U.S. forums such as Patriots.win and Greatawakening.win.[3] The truth was that Cloutier had not been in Ukraine since July 2021. Additionally, the rumor mistook Cloutier's rank, which was Lieutenant General and the commander of NATO's Allied Land Command, instead of "Major General."[4]

This false claim was disseminated not only in the U.S. but also in Europe in different languages.[5] It also soon appeared on Chinese social media and video

2 Craig Silverman, Jane Lytvynenko, and William Kung, "Disinformation For Hire: How A New Breed Of PR Firms Is Selling Lies Online," BuzzFeed News, January 2020, https://www.buzzfeednews.com/article/craigsilverman/disinformation-for-hire-black-pr-firms.

3 Bill McCarthy, "Social Media Users, Far-Right Websites and QAnon Internet Forums Falsely Claimed That Lt. Gen. Roger Cloutier, Commander of NATO's Allied Land Command, Was Captured by Russian Forces in Ukraine. 'Completely False,' an Allied Land Command Spokesperson Said.," @Politifact, April 5, 2022, https://www.politifact.com/factchecks/2022/apr/05/tweets/no-nato-allied-land-command-leader-wasnt-captured-/.

4 Ibid.

5 Maldita, "No, el ejército ruso no ha capturado al militar estadounidense Roger Cloutier en Mariupol (Ucrania)," Maldita.es, April 2022, https://maldita.es/malditobulo/20220411/ejercito-ruso-capturado-estadounidense-mariupol/.

platforms, such as Weibo and Xigua Video (西瓜视频), as well as social media popular among Taiwanese and overseas Chinese speakers, like Facebook and LINE.[6] Moreover, the Chinese claim added more untrue elements to the original one, asserting that the UK media, BBC, had reported that Russia had denied the UK and U.S. requests to release the "Major General".[7] Since then, several pieces of false information circulated on Chinese-language platforms claimed that several NATO high-ranking officers had been captured in Ukraine, but the information pieces contained different details. For example, one piece spread in Taiwan stated that the Taiwanese media buried the news that more than 50 high-ranking NATO and other allies' commanders had been captured and sent to Russia for trial.[8]

The above disinformation pieces of the same claim propagated throughout Europe, North America, Asia, etc. Nonetheless, they catered to a variety of audiences and sentiments. In Europe and the U.S., such assertions were exploited to weaken Europe and the United States' support for Ukraine, while in Taiwan, the pieces were meant to instill suspicion in the media and doubt in the strength of the U.S. and NATO.

It was difficult, though, to attribute who was responsible for initiating the disinformation and distinguish which propagators were associated with authoritarian governments. However, the above example (and still many others we have witnessed in recent years) demonstrates how rapidly similar false statements can cross national borders, be amplified and altered by different

6 "【錯誤】網傳「北約歐洲司令被俄羅斯俘虜,美英求俄羅斯放人被拒」[False: the online rumor that the NATO European Commander was captured, Russia denied UK and US's request to release the hostage]," Taiwan FactCheck Center, April 2022, https://tfc-taiwan.org.tw/articles/7188.

7 Ibid.

8 "【錯誤】網傳影片「鋼鐵廠大魚全部投降 放押往俄羅斯審判!五十多名北約或其他國家 高級指揮官全部被俘虜」、「為什麼台灣的電視新聞台都沒有播報?包含現役美軍中將三顆星, 少將兩顆星。以及北約的諸多大員, 活捉耶!新聞播報的偏取向」[False: All the big fish from the steel factory surrendered and were taken to Russia for trial! More than 50 senior commanders from NATO or other countries were all captured. Why didn't Taiwan's TV news stations broadcast it? Are they biased? Three-star active US military lieutenant generals, two-star major generals, and many NATO officials were captured alive!]," Taiwan FactCheck Center, July 2022, https://tfc-taiwan.org.tw/articles/7506.

propagators, and target audiences in different geographic regions with varying results. It also showcases how false claims can have far-reaching consequences and highlights the need for democratic countries to work together in the battle against disinformation campaigns carried out by authoritarian regimes.

Lessons Learned

The aforementioned example also highlights a number of difficulties democratic countries confront in tackling the disinformation. We dissect the problems by employing the framework of the communication process, including senders, messages and channels, and audiences, to identify the challenges.

1. ***Senders of Disinformation:***

   As we have mentioned previously, it is always difficult to identify the creators or initiators of disinformation campaigns. Take the "NATO commanders have been captured" disinformation as an example. It is hard to pinpoint whether Russia or right-wing sympathizers in Western countries launched these disinformation pieces. It is also difficult to establish whether the Chinese propagators who translated the false claims into Chinese and shared them on social media were affiliated with the government or were simply Chinese extreme nationalists.

   However, throughout the years, non-governmental groups like think tanks and fact-checking programs, social media and technology companies, and government agencies tasked with handling misinformation concerns have accrued knowledge and experience about the disinformation ecosystem. Many of them have created significant reports and databases that identify bad actors and map the paths and hubs of disinformation dissemination. The expertise and databases would be helpful in identifying the patterns and signs of disinformation operations.

2. ***Messages and Channels of Disinformation:***

   From a communication process viewpoint, disinformation, like other categories of information, needs "channels" and intermediaries to deliver messages. In the digital age, these intermediaries include, but are not

limited to, social media, mainstream media, online websites and forums, and individuals such as politicians and celebrities. The speed and scope of disinformation hinges on how many and how effective the message channels are.

a. *Social media*: Studies have demonstrated that social media algorithms speed up and amplify more false information than benign content.[9] As we have seen from the Ukraine War disinformation example and many others, messages posted and spread in English on X or Facebook were soon introduced to Chinese social media platforms. The Internet connection, the social media algorithms that favor shocking information, and the availability of online translation tools have benefited the disinformation pieces to overcome language barriers and prevail globally in different languages quickly.

   Apparently, social media platforms should and have been crucial allies in the global effort to counter disinformation. During the COVID-19 pandemic, the 2020 U.S. presidential election, and the January 6 United States Capitol attack in 2021, social media companies indeed played a role in limiting the dissemination of harmful information. However, the positive engagement of social media companies in defeating disinformation took a sharp turn in 2023 due to economic downturns in the technology industry, growing accusations of censorship toward content moderation from political camps, and the ownership transition of X (formerly known as Twitter).

   As a result, 2023 has seen multiple layoffs of social media companies' internet trust and safe teams and staff in charge of content moderation.[10]

---

9 Jeff Allen, "Misinformation Amplification Analysis and Tracking Dashboard — Integrity Institute," Integrity Institute, October 2022, https://integrityinstitute.org/blog/misinformation-amplification-tracking-dashboard.

10 Hayden Field and Jonathan Vanian, "Tech Layoffs Ravage the Teams That Fight Online Misinformation and Hate Speech," *CNBC*, May 26, 2023, https://www.cnbc.com/2023/05/26/tech-companies-are-laying-off-their-ethics-and-safety-teams-.html.

Several platforms have also relaxed their policies or reinstated controversial accounts.[11] Moreover, companies such as Meta and X have made it more difficult for researchers to access the platforms' data to track the flow of disinformation. Although these companies claimed that there are alternatives to the old false information monitoring tools, observers have noted that these tools or programs are unaffordable to many researchers or restricted in functions compared with old ones.[12]

b. *Mainstream media*: We have seen several examples of major media outlets amplifying disinformation, especially when the information pieces cover global news events and use foreign sources. A recent example was Taiwanese media reporting an unfounded remark by American far-right personality Dom Lucre about the identity of the shooter who attempted to assassinate Trump at an election campaign event in July 2024.[13] Lucre falsely claimed on X that a female sitting behind Trump at a speech could be an FBI agent who secretly gave the shooter instructions to shoot Trump. Taiwanese online outlets relayed this message without questioning the accuracy of the material or reminding readers of Lucre's credibility. As a result, this inaccurate message from an American far-right activist influenced Taiwanese audiences' perceptions of American politics.

Of course, many factors contribute to Taiwanese flawed international news coverage, such as an overly competitive media climate and a lack of fact-checking resources. However, many global media institutions have faced similar problems of dwindling resources for international news reporting.[14]

---

11 Kari Paul, "Reversal of Content Policies at Alphabet, Meta and X Threaten Democracy, Warn Experts," *The Guardian*, December 7, 2023, https://www.theguardian.com/media/2023/dec/07/2024-elections-social-media-content-safety-policies-moderation.

12 Casey Newton, "How CrowdTangle Predicted the Future," Platformer, March 2024, https://www.platformer.news/meta-crowdtangle-shutdown-dsa-platform-transparency/

13 Wei-Ping Li, "The Internet as an Unreliable Witness Rumors in Taiwan and the Chinese-Language Media Regarding the Attempted Assassination of Trump," Taiwan FactCheck center, August 2024, https://tfc-taiwan.org.tw/articles/10904.

14 Bill Gentile, "With Foreign Bureaus Slashed, Freelancers Are Filling the Void – at Their Own Risk," American University, January 2019, https://www.american.edu/soc/news/with-foreign-bureaus-slashed-freelancers-are-filling-the-void-at-their-own-risk.cfm.

Without sufficient news sources, local mainstream media might even turn to sources from untrustworthy social media when important global events like wars or natural disasters arise. The decline of mainstream media's resources in international reporting thus provides sufficient opportunity for malevolent actors to spread disinformation across national borders.

c. *Politicians and celebrities*: While authoritarian countries have been the primary perpetrators of disinformation operations, certain politicians and celebrities in democratic countries have also participated in the communication process by echoing and amplifying authoritarian governments' narratives. This does not mean that these politicians or celebrities are associated with the authoritarian governments behind information campaigns. However, politicians and celebrities may unintentionally engage with or promote disinformation since the messages underlying the disinformation pieces align with their interests. Evidence has indicated that Russian influence campaign operatives have exploited American politicians or political influencers to undermine the public's support for the Russia-Ukraine war by engaging the social media accounts of American politicians and taking advantage of their massive followers.[15]

3. *Audiences of Disinformation:*

The ultimate goal of disinformation campaigns is to influence audiences in the target countries. In the digital age, viewers are constantly overwhelmed with large amounts of information, leaving little time to assess its accuracy. When information or news coverage is about faraway events, audiences have even fewer sources to check the accuracy. To make matters worse, the design of social media platforms has made it easy for viewers to share material with a few clicks on a phone or tablet. Because of audiences' vulnerability, social media platforms, traditional media sources, and political influencers that serve as information channels and intermediates are even more vital in assuming the responsibility of

15 Alexa Corse, Dustin Volz, and Carlos Barria/Reuters, "How Russian Trolls Are Trying to Go Viral on X," *Wall Street Journal*, August 21, 2024, https://www.wsj.com/politics/national-security/russian-trolls-x-twitter-1e993a31.

information safeguards. On the other hand, audiences should take a more active role in improving their media literacy to recognize problematic information.

To summarize, based on the communication framework, we identify the following issues when democratic countries confront disinformation attempts from authoritarian regimes: 1. There are difficulties in determining the schemes and initiators of disinformation campaigns; 2. The internet and social media have increased the spread of disinformation across boundaries. However, social media companies have withdrawn from the frontlines of combating foreign disinformation; 3. Mainstream media and political influencers have unwittingly or purposefully promoted foreign disinformation; and, 4. Audiences have fewer resources for detecting and being alert to foreign disinformation attacks.

Strengthen International Collaboration to Safeguard Democracy and Civil Society

To address these problems, we believe that more cooperation among democratic countries and cross-sectoral collaborations can help combat disinformation campaigns conducted by authoritarian regimes. As previously stated, disinformation spreads across boundaries and is exploited by various actors. A concerted effort by democratic countries will improve all the allies' ability to detect, warn, and prevent the spread of misinformation.

Here, we recommend two major paths to achieve the collaboration:

1. ***More cross-sectoral collaboration in regions and among continents***

a. **Involve more sectors in the collaboration:**
Many disciplines, including geopolitics, national security, technology, information production, and psychology, are involved in campaigns against disinformation. These campaigns also require cooperation from various sectors, including news organizations, governments, non-governmental organizations, technological firms, academic institutions, and even individual

influencers. Additionally, more opportunities should be provided for stakeholders in various fields to share resources, expertise, and experiences.

b. More frequent collaborations among regions and countries:
Collaborations among regions and countries could help to issue early warnings of disinformation attacks or quickly deter the flow of disinformation. In recent years, civil society has responded to international emergencies with prompt cross-border alliances. For instance, the signatories of the International Fact-Checking Network (IFCN) quickly established the CoronaVirusFacts Alliance during COVID-19, bringing together fact-checking groups from over 110 countries to gather false information about the pandemic and disseminating fact-checking reports in 40 languages.[16] Through this partnership, the dissemination of incorrect information was made more widely known, fact-checkers received increased support from their peers in the global community, and the task of fact-checking was made easier. Moreover, the false information collected in the CoronaVirusFacts Alliance has provided important data for researchers to study the transnational flow of false information.

The CoronaVirusFacts Alliance project came to an end in 2023. It has set an ideal example for cross-border cooperation. However, initiatives such as this global cooperation ought to be expanded into an ongoing program. False information, after all, does not end in a single incident. The EU has established the East Stratcom Task Force to counter Russia's disinformation campaigns.[17] Currently, NATO has established a platform, the Strategic Communications Centre of Excellence, to enhance strategic communications among NATO allies and its partners and monitor information manipulations.[18] The intergovernmental and

16 The Poynter Institute, "CoronaVirusFacts Alliance - Poynter," Poynter, November 2023, https://www.poynter.org/coronavirusfactsalliance/.

17 "Questions and Answers about the East StratCom Task Force," EEAS, n.d., https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en#11232.

18 "StrATCOM | NATO Strategic Communications Centre of Excellence Riga, Latvia," n.d., https://stratcomcoe.org/about_us/about-nato-stratcom-coe/5.

non-governmental projects may serve as models for democratic countries in other regions looking to develop alliances and exchange information. In addition, given that technology has made it easier for disinformation to traverse linguistic and geographical boundaries, establishing cross-continental cooperation will be much more crucial.

2. *Leverage international principles and consensus to prompt positive reforms*

One significant advantage of international cooperation is that it can grow into a powerful force, facilitating positive reforms or changes. We believe that collaborative global efforts to develop guidelines for combating disinformation could help push social media companies to reinvest more resources in the fight against disinformation influences. On the other hand, the guidelines can serve as a blueprint for countries to undertake domestic legal and policy reforms on content moderation addressing disinformation.

The Santa Clara Principles on Transparency and Accountability in Content Moderation, developed by non-governmental groups, are one example of international civil society collaboration that has resulted in positive changes in platform policy. As the name implies, the *Principles* are founded on global human rights principles and incorporate the *United Nations Guiding Principles on Business and Human Rights* recommendations. The *Santa Clara Principles* outline standards of transparency and due process that platforms ought to meet to provide accountability for handling user-generated content.[19]

According to the Santa Clara Principles documents, at the time when the *Principles* were established, technology companies gave relatively little information about "the scope, scale, and impact of internet platforms' content moderation efforts."[20] Nonetheless, since the *Principles*'

19 "Santa Clara Principles," Santa Clara Principles, n.d., https://santaclaraprinciples.org/history/.

20 Ibid.

introduction in 2018, technology giants such as Apple, Facebook, GitHub, Google, Instagram, LinkedIn, Medium, Reddit, Snap, Tumblr, Twitter, and YouTube have pledged to adhere to the *Principles*.[21] In addition, the *Principles* have also been an important benchmark for the evaluation of legislation regarding content moderation.[22]

Based on the Santa Clara Principles model, the international community should continue developing principles on content moderation. Currently, disinformation campaigns from authoritarian regimes have posed a significant threat to democratic countries. However, platforms have retreated from their previous efforts in content moderation, while democratic countries have struggled to strike a balance between free expression and combating harmful disinformation content. At this point, it may benefit the international community to more actively engage in discussions on developing human-rights-based international principles to address disinformation challenges.

21 Ibid.

22 "Unravelling the Digital Services Act Package," European Audiovisual Observatory, 2021, https://rm.coe.int/iris-special-2021-01en-dsa-package/1680a43e45.

10. The Evolution of Information Warfare: Russia and China's Strategic Partnership

Niklas Swanström and Filip Borges Månsson

In today's digital age, the manipulation of information has become a cornerstone of modern statecraft, with Russia and China emerging as dominant forces in shaping the global information landscape. While their methods and objectives differ, their growing collaboration in disinformation campaigns poses an unprecedented challenge to liberal democracies worldwide. This partnership, ranging from coordinated narrative amplification to the exploitation of societal divisions, represents more than mere tactical alignment—it signals a broader strategic effort to erode Western influence and reshape the international information order. The editors' assessment of the chapters in the book has been summarized in six broad policy recommendations below that we think is necessary to take into consideration to ensure a more effective counter policy against dis- and mis-information:

Policy Recommendations

1. Strengthening Information Resilience

- Develop transnational networks for countering disinformation
- Enhance cooperation among intelligence agencies, tech companies, and civil society
- Expand frameworks like NATO's StratCom Center of Excellence to include non-NATO partners

2. Digital Literacy and Public Awareness

- Invest in comprehensive digital literacy programs

- Create educational campaigns focused on manipulation tactics
- Foster collaboration between academia, tech sector, and government agencies

3. *Technological Solutions*

- Leverage AI and machine learning for early detection of disinformation
- Develop transparent content moderation systems
- Balance security measures with privacy and free speech

4. *Legal and Regulatory Framework*

- Update platform regulations to address modern disinformation challenges
- Mandate transparency in content sourcing and state-sponsored content
- Establish clear accountability measures for tech companies

5. *Strategic Communication*

- Proactively shape information environments with accurate narratives
- Counter anti-Western propaganda through targeted messaging
- Focus on vulnerable regions in Eastern Europe and Southeast Asia

6. *International Cooperation*

- Engage non-aligned states in information integrity initiatives
- Provide technical assistance and share best practices
- Build broader coalitions against authoritarian influence

In this volume, we have delved into various perspectives and insights that stem from the fact that the evolving partnership between Russia and the People's Republic of China (PRC) presents a profound challenge for liberal democracies in the realm of disinformation. Apart from the broad policy recommendations that we present based on these insights, some key points can be considered based on the various perspectives introduced:

Foundations of Cooperation

The Russia-China partnership in disinformation stems from pragmatic necessity rather than ideological alignment. Russia's aggressive disinformation tactics complement China's more calculated, image-conscious approach, creating a formidable synergy despite their divergent core interests. While Russia focuses primarily on European affairs and China on the Asia-Pacific region, both nations find common cause in opposing U.S. hegemony and Western democratic values.

Their distinct methodologies—Russia's disruptive strategies and China's emphasis on self-promotion and information control—showcase the sophistication of their combined efforts. This cooperation, though largely opportunistic, proves most effective in low-cost, high-impact operations that align with both nations' strategic interests. The relationship's pragmatic nature became particularly evident during Russia's invasion of Ukraine, where China amplified Russian narratives while carefully avoiding direct military involvement.

Technological Enhancement and Institutional Framework

Advanced technology has dramatically expanded both nations' capabilities in information operations. Russia has mastered social media manipulation, cyber operations, and traditional propaganda techniques, while China's technological infrastructure, particularly in AI, enables increasingly sophisticated methods of controlling information flows and shaping global narratives. The integration of emerging technologies—including automated systems, deepfake technology, and AI-driven content generation—has not only enhanced campaign efficiency but also complicated traditional countermeasures.

This technological convergence extends into institutional frameworks through forums like the Shanghai Cooperation Organisation (SCO) and BRICS, where both nations align their strategies on information control and cyber governance. These platforms advance concepts like "internet sovereignty" that justify state censorship and digital control, while facilitating the exchange of tactics and regulatory approaches to restrict digital freedoms.

While Russia and China continue to refine their information operations, the international community struggles to keep pace with the rapidly evolving landscape of digital manipulation. The integration of advanced technologies enables disinformation campaigns to be conducted at unprecedented speed and scale. This underscores the need for a more proactive approach to public resilience, one that includes fostering a culture of critical digital literacy and enhancing cross-sector collaboration to rapidly identify and respond to threats.

Domestic Control and External Projection

The effectiveness of Russian and Chinese disinformation campaigns stems partly from their robust domestic information control systems. Russia's hybrid media landscape and China's centralized media environment enable both regimes to maintain strict control over information flows. This domestic control extends internationally through state-affiliated outlets like RT, Sputnik, Xinhua, and CGTN, which work in concert to saturate global information spaces with coordinated narratives that challenge Western perspectives. The integration of traditional media, online platforms, and covert social media activities enables a seamless blending of disinformation into public discourse abroad. This dual approach allows them to adjust their narratives for different target audiences, shifting between outright propaganda and more subtle forms of persuasion. By leveraging state-affiliated outlets and a network of proxies, both nations saturate the global information environment, pushing narratives that destabilize adversaries and amplify internal divisions.

Divergent Interests and Strategic Tensions

Despite their cooperation, fundamental differences in strategic interests and approaches create potential friction points. In Central Asia, for instance, China's expanding economic influence through the Belt and Road Initiative challenges Russia's traditional sphere of influence, leading to competing regional narratives. Their approaches to international law and institutions also differ significantly: China typically works within existing frameworks to reshape global norms, while Russia often adopts a more overtly disruptive stance.

Resource disparities further differentiate their approaches. Russia's economic constraints foster reliance on cost-effective tactics like social media manipulation and cyberattacks. In contrast, China's substantial resources enable more sophisticated, sustained campaigns leveraging advanced technologies and data analytics. This technological asymmetry influences the depth and nature of their collaboration, particularly in sensitive areas like cyber capabilities.

The Role of Ideological Flexibility

Both nations demonstrate remarkable ideological adaptability in their information operations, allowing them to tailor messages for different audiences and contexts. It also allows for Russia and China to exploit shifting geopolitical trends and public sentiments more effectively, making their disinformation strategies more resilient and difficult to counter. Russia's ability to simultaneously support various ideological movements complements China's development-focused messaging. However, this flexibility can backfire when narratives evolve beyond their originators' control, as witnessed with COVID-19 misinformation and anti-vaccine campaigns.

Conclusion

The convergence of Russian and Chinese disinformation represents a sophisticated challenge to democratic societies. While their partnership remains pragmatic rather than ideological, their combined capabilities pose a significant threat to the international information order. Effective countermeasures require a nuanced understanding of their individual strategies and cooperation dynamics, coupled with a comprehensive approach that combines technological innovation, policy reform, and international collaboration. Success in this endeavor is crucial for preserving the integrity of democratic discourse and maintaining a rules-based international order.