CHARLES UNIVERSITY

FACULTY OF SOCIAL SCIENCES

Institute of Political Studies

Department of Security Studies

Master's Thesis

2022 **Atandra Ray**

CHARLES UNIVERSITY

FACULTY OF SOCIAL SCIENCES

Institute of Political Studies

Department of Security Studies

Disinformation and Propaganda as Tools of Influence in Cyber Space: How do Chinese information operations differ from the Russian ones? In what way are they similar and in what way are they different and why?

A Comparative Case Study of China and Russia

Master's Thesis

Author: Atandra Ray

Academic supervisor: David Erkomashvili, Ph.D.

Study programme: International Security Studies (MISS)

Year of submission: 2022

DECLARATION OF AUTHENTICITY

I herewith declare that I wrote this thesis on my own and did not use any unnamed sources or aid. Thus, to the best of my knowledge and belief, this thesis contains no material previously published or written by another person except where due reference is made by correct citation. This includes any thoughts taken over directly or indirectly from printed books and articles as well as all kinds of online material. It also includes my own translations from sources in a different language. The work contained in this thesis has not been previously submitted for examination. I also agree that the thesis may be tested for plagiarized content with the help of plagiarism software. I am aware that failure to comply with the rules of good scientific practice has grave consequences and may result in expulsion from the programme.

In Prague 02/08/2022 Atandra Ray

KEYWORDS

Information operations, Disinformation, Russia, China, Influence Operations, Hybrid Warfare, Social Media

TITLE

Disinformation and Propaganda as Tools of Influence in Cyber Space: How do Chinese information operations differ from the Russian ones? In what way are they similar and in what way are they different and why?

1 Introduction

Information is a vital instrument for waging war against an adversary. In the past, information was utilised as an addition to the element of physical warfare. In the modern era, winning the informational aspect is as important as winning the physical one **(Pomerantsev, 2015)[1].** The term hybrid warfare has been utilised extensively in security studies and international relations-related discourse since the Russian annexation of Crimea in 2014. When distilled from the inherent vagueness surrounding the definition of hybrid warfare, it can be opined that hybrid warfare is a mix of conventional and unconventional means of warfare, often utilising the tools of deception, sabotage and disinformation **(Maschmeyer, 2021)[2].**

Through disinformation, hybrid warfare permeates not only military personnel but also affects ordinary civilians who are not in an active zone of conflict **(Katz, 2021)[3]**. For instance, during the 2016 U.S. elections, Russia exploited the so-called digital battlefield using online influence operations, also broadly known as information operations, which led to the broader dissemination of propaganda **(Pollock, 2017)[4]**. The sophistication of the Russian interference in the 2016 United States elections was further elaborated upon by the U.S. Director of National Intelligence, who stated that Russian President Vladimir Putin ordered an influence campaign to undermine the public trust in the U.S. presidential election. Most of this influence campaign was orchestrated through both covert and overt intelligence efforts, with the former

[1] https://www.theatlantic.com/international/archive/2015/12/war-2015-china-russia-isis/422085/
[2] https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse278-EN.pdf
[3] https://international-review.icrc.org/articles/protecting-civilians-from-disinformation-during-armed-conflict-914
[4] https://www.technologyreview.com/2017/04/13/152305/russian-disinformation-technology/

focused more on cyber propensities leading to the use of troll farms and hacking, and the latter more focused on actions undertaken by the Russian state-affiliated media agencies and third-party intermediaries **(U.S. Office of the Director of National Intelligence, 2017)**[5].

The People's Republic of China (PRC) has been perpetuating its version of the informational aspect of the war against adversaries. It's not a coincidence that Soviet activities have partly inspired Chinese influence operations. The Chinese way of information warfare draws on the United Front (统一战线) and the well-rounded Three Warfares strategy (三种战法), which involves exploiting the means of legal, psychological, and media warfare to help achieve an abundance of ambitions. Beijing has notoriously used the Three Warfares strategy in the disputed region of the South China Sea. The South China Sea has significant geostrategic importance as it is home to resources worth 5 trillion dollars, including energy reserves and shipping lines. China's claims in this territory overlap with those of its neighbours which include but are by no means limited to the Philippines and Vietnam **(Pomerantsev, 2015)**[6].

Throughout the COVID-19 pandemic, Beijing has utilised an information offensive featuring disinformation about the origin of the coronavirus – such as the leading conspiracy theory that the virus originated from a bioweapon's lab located in the

[5] US Office of the Director of National Intelligence, "Background to "Assessing Russian Activities and Intentions in Recent US Elections," The Analytic Process and Cyber Incident Attribution," 06 January 2017, https://www.dni.gov/files/documents/ICA_2017_01.pdf.
[6] https://www.theatlantic.com/international/archive/2015/12/war-2015-china-russia-isis/422085/

United States of America. To make sure that this narrative was strengthened, Beijing circulated this claim through its internal information ecosystem and further dispensed it by using high-profile diplomats on social media that have a high reach of followers **(Rosenberger, 2020)**[7]. In fact, the broader consensus around misinformation, as well as disinformation, led to scholars describing the COVID-19 pandemic as an infodemic. Infodemic is described as the overabundance of information, part of which is accurate, and part of which is inaccurate, occurring during the times of an epidemic **(Venkataramakrishnan**[8]**, 2020)**.

In the 21st century, state-sponsored propaganda and disinformation take shape across a spectrum of domains. Social media is becoming an important conduit for the authoritarian dissemination of disinformation. At a time when the consumption of news is increasingly becoming digital, manipulation of public opinion over social media is becoming a danger to public life. The realm of social media acts as an important catalyst when it comes to the polarization of political discourse. The COVID-19 pandemic has illustrated a broad domain of threats regarding the production and dissemination of accurate information. Over the past few years, the pandemic has made it clear that ensuring everyone is well-informed is becoming challenging **(Seger, 2021)**[9]. During a crisis, science can be forced into the media spotlight. For instance, despite having no credible evidence that COVID-19 was

[7] https://www.foreignaffairs.com/articles/china/2020-04-22/chinas-coronavirus-information-offensive
[8] https://www.ft.com/content/e5954181-220b-4de5-886c-ef02ee432260
[9] https://www.bbc.com/future/article/20210209-the-greatest-security-threat-of-the-post-truth-age

bioengineered in a lab, disinformation was pushed forth by state and non-state actors for their gains **(Cohen, 2020)**[10].

The ongoing Russian invasion of Ukraine in 2022 provided pieces of evidence pertaining to the amplification of the Kremlin's propaganda and disinformation machinery by Beijing. For instance, Beijing echoed a Russian conspiracy theory that the U.S. military is operating hazardous biolabs in Ukraine. This piece of disinformation was similar to the time when the CCP accused the U.S. of bioengineering COVID-19 in Fort Detrick, a U.S. military facility located in Maryland **(Glamann, 2022)**. The Global Information Operations Threat Intel Lead at Meta, Ben Nimmo, states that "In Russia and China, information warfare is seen as a permanent activity which is to be practised regardless of the absence of immediate conflicts, open-ended and widely applicable" **(Legatum Institute, 2015)**.[11]

Both China and Russia have a tendency to utilise information operations against their domestic population. According to the Oxford Internet Institute (OII), in democracies, information operations were utilised by non-state groups to target the domestic populace, whereas, in authoritarian states, the state itself targets its own populations to keep them in line with the broader state propaganda **(Bradshaw, Howard, 2017)**[12]. When it comes to China, numerous scholars, activists, and journalists call this process astroturfing. In doing so the Chinese government hires social media commentators known as the '50 cent army' (五毛党) to fabricate

[10] https://www.science.org/content/article/scientists-strongly-condemn-rumors-and-conspiracy-theories-about-origin-coronavirus
[11] https://li.com/reports/information-at-war-from-chinas-three-warfares-to-natos-narratives/
[12] https://ora.ox.ac.uk/objects/uuid:cef7e8d9-27bf-4ea5-9fd6-855209b3e1f6

comments making it look like they were written by common Chinese citizens. **King, Pan, Roberts, 2017)**[13].

2 Methodology

In the pursuit of a comprehensive understanding of Russian and Chinese information operations in the Contemporary Era, the dissertation's methodology is carried out in the form of case studies. This thesis will employ a cross-case analysis, in which the researcher studies multiple cases, accumulates knowledge and understanding of the individual cases, compares and contrasts their qualities, and produces new knowledge based on interpretive qualitative analysis. To understand how each regime utilises information operations this thesis will look into several components of the authoritarian information operations environment. To provide analysis into information operations as perpetrated by the Kremlin, the ongoing Russo-Ukrainian war since 2014 will be taken into account. To provide an analysis of Beijing's way of disseminating key narratives, the thesis will analyse the role of the exhaustive machinery of disinformation employed by the CCP during the emergence of the COVID-19 pandemic. Even though the research in this thesis concentrates on the most recent developments in the context of information operations undertaken by the two authoritarian states, the timeline of the analysis covers the period between 2014 and to present.

[13] https://www.cambridge.org/core/journals/american-political-science-review/article/how-the-chinese-government-fabricates-social-media-posts-for-strategic-distraction-not-engaged-argument/4662DB26E2685BAF1485F14369BD137C

3 Literature Review

The literature used in this thesis will be segmented into different blocks of information. The first segment will lay down the foundation of the different kinds of the terminology used during the course of the thesis. The literature review will start with the definition of crucial keywords that make the thesis authoritative - information operation and disinformation - that have their own meanings and interpretations around the world and are contested for prominence with regards to their definition as that varies considerably.

.

When it comes to Russia, this thesis will consult sources formulated by various government bodies as well as think tanks in the West that have had prolonged exposure to countering and have done extensive policy-oriented research and analysis on Russian information operations. For instance, the NATO Strategic Communications Centre of Excellence (StratCom CoE), the Atlantic Council's Digital Forensic Lab, the RAND Corporation, the Netherlands-based investigative journalism group known as Bellingcat and the University of Toronto's Citizen Lab. It is hard to understate the investigations carried out by publications such as New York Times, Wired, the Financial Times and the Washington Post and therefore existing literature will be utilizing knowledge from these sources as well for secondary research.

When it comes to China, this thesis will draw on open-source Chinese-language research done by Western experts in the influence operations field. Since Taiwan is a victim of a myriad of influence operations from China, social media reports and

commentary from Taiwanese publications will be borrowed such Taiwan based Doublethink Lab which works on researching malign Chinese influence operations and disinformation campaigns. Considering that a lot of government bodies in the West are slowly taking the threat of China's influence operations seriously, this thesis will look at reports from think tanks that have done extensive research on Chinese influence operations such as the Internet Observatory Cyber Policy Center at Stanford University, the RAND Corporation, Brookings and the Institute for Strategic Research at the Military School (IRSEM).

3.1 What are information/influence operations?

Progress on the issue of the conceptual underpinnings of information operations remains inadequate and insufficient with fierce scholarly confrontations raging over definitions. When it comes to the definition of homogeneous terms that are used together in the broader scope of scholarly debate such as Information Warfare, Psychological Operations, and Influence Operations there is a lot of confusion, these terms are used in different contexts and have a tendency of changing given the purpose and action of their usability. This is precisely why it is important to highlight and elucidate the definitions. Since this thesis will primarily look at the role of information operations through the lens of 'foreign actors', attribution of said actors as such is essential, which is difficult to formulate considering that it involves questions such as 'How relevant is a country's legal definition of foreign to determining how acceptable a participant is in public debate?' or 'How does one account for proxy or sympathetic actors ('useful idiots') who may be persuaded or coerced into supporting the goals of a foreign state?' among others **(Wanless,**

Pamment, 2019)[14]. The idea of foreignness leads to various philosophical questions that don't necessarily have a black or white definition. Therefore, the definition of information operations will lay emphasis on the military applicability of undertaking such an operation as well as the civilian rhetoric as well.

The U.S. Department of Defense (DoD) definition of Information Operations underlines it as a military capability by stating that information operations refer to 'the integrated employment, during military operations, of information-related capabilities in concert with other lines of operations to influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting its own'. **(U.S. DOD, 2013)**[15]

This thesis will also rely on the definition of information operations utilized by social networking organizations such as Facebook for instance. Facebook's security team defines information operations as 'actions taken by governments or organized non-state actors to distort domestic or foreign political sentiment, most frequently to achieve a strategic and/or geopolitical outcome. These operations can use a combination of methods, such as false news, disinformation, or networks of fake accounts (false amplifiers) aimed at manipulating public opinion.' For Facebook, the definition of information operations moves beyond the conventional military overview

[14] https://carnegieendowment.org/2019/12/30/how-do-you-define-problem-like-influence-pub-80716
[15] US Department of Defense, Directive 3600.01. May 2, 2013. p.12

and revolves more around the phenomenon of shaping the information environment. **(Weedon, Nuland & Stamos 2017, p. 4)**[16]

3.2 How do we differentiate between information operations and influence operations?

Despite their similarities, the two techniques have been defined separately. The RAND Corp for example chose to stick with a broader perspective on the definition of influence operations, "efforts to influence a target audience, whether an individual leader, members of decision-making group, military organizations and personnel, specific population subgroups, or mass publics".[17] **(Wanless, Pamment, 2019)**

However, it is important to move beyond the more military-based traditional confinements of the definition of influence operations as influence operations are not limited to military operations anymore, but can be part of influencing the behaviour of the targeted audience in peacetime through the diplomatic arena or during armed conflict. Therefore, in the approach of this thesis, Information Operations are a subset of Influence Operations as it broadly encompasses a variety of definitions to influence the targeted audience **(Brangetto, Veenendaal, 2016).**[18]

---

16 https://i2.res.24o.it/pdf2010/Editrice/ILSOLE24ORE/ILSOLE24ORE/Online/_Oggetti_Embedded/Documenti/2017/04/28/facebook-and-information-operations-v1.pdf

17 https://carnegieendowment.org/files/2020-How_do_you_define_a_problem_like_influence.pdf

18 https://ccdcoe.org/uploads/2018/10/Art-08-Influence-Cyber-Operations-The-Use-of-Cyberattacks-in-Support-of-Influence-Operations.pdf

3.3 How can we define disinformation campaigns?

Journalists, commentators, decision-makers, and academics have used a number of terminologies to describe the accuracy and significance of media content such as propaganda, disinformation, misinformation, and so on. However, these wordings do carry a significant obstacle as each of them tends to blend into the interpretation and context of a particular cultural annotation or a historical meaning. To make sure that the definitions are easier to interpret, this thesis will be referring to a report published in the year 2017 by the Council of Europe (COE) titled 'Information disorder: Toward an interdisciplinary framework for research and policy making' that provides a new framework for people working on the theoretical and practical challenges related to both mis and disinformation.

Disinformation is therefore defined by this particular publication as "Information that is false and deliberately created to harm a person, social group, organization or country," whereas misinformation is referred to as "Information that is false, but not created with the intention of causing harm." **(Wardle, Derakhshan, 2017)**[19] Disinformation gained prominence during the 2016 U.S. Presidential Elections which led to the rise of "fake news" as terminology to describe disinformation, the interchangeability led to noteworthy challenges. For instance, fake news was politicized by political elites to undermine trust in the media industry **(European Commission, 2018)**.

[19] https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html

The use of propaganda is a central element of disinformation campaigns. Professor Nicholas O'Shaughnessy, an Emeritus Professor of Communication at Queen Mary, University of London, states that "all propaganda is not disinformation but… all disinformation is propaganda" **(Bradshaw, 2020)**[20]. Propaganda doesn't have a particular political connotation to it. The word has a lot of commercial advertising and public relations utility as well. For example, propaganda can be used by states during democratic processes as a means of exerting influence, propaganda can also be utilized by a corporate firm for manipulating market opinion to make circumstances more profitable for them. The scope of this thesis however is well within the realms of political science which means that every terminology that is defined here will be used as such in that realm.

3.3.1 The evolution of information operations and disinformation campaigns from analogue to digital

The word disinformation takes its root from the practice of dezinformatsiya used by the Soviet Union's intelligence agencies. The word dezinformatsiya was formulated in the year 1923 when the Disinformation Bureau, also known as Dezinformburo, was approved by the Soviet Security Service within the Politburo. The primary intention of the Dezinformburo was to manufacture the falsehood that the Soviet economy was doing much better than that of its Western counterparts, along with showcasing how the Red Army was more combat-ready than it actually was **(Tolz, Hutchings, 2021)**[21].

[20] https://ora.ox.ac.uk/objects/uuid:e75e4796-d614-454b-b2e2-df6b8659e610
[21] https://blogs.lse.ac.uk/medialse/2021/10/08/performing-disinformation-a-muddled-history-and-its-consequences/ - Performing disinformation: a muddled history and its consequences

The roots of perhaps the first disclosed active measures disinformation campaign against the west can be traced back to the Soviet Union in the 1980's, also known as Operation INFEKTION.[22] According to KGB defector Ilya Dzerkvelov, in the '60s, the pro-Soviet Indian newspaper Patriot was set up for the solitary purpose of publishing disinformation. The myth that HIV/AIDS had been produced as part of a biological weapons research project at Fort Detrick in the United States by genetic engineers was first published by Patriot. The pro-Soviet Indian newspaper published a front-page article with the headline and the sub-headline as the following: "AIDS may invade India: Mystery disease caused by U.S. experiments." The KGB eventually attributed the U.S. biological weapons research project responsibility by citing the disinformation published earlier by the Patriot in an article titled "Panic in the West, or what is hiding behind the sensation surrounding AIDS" published by the Soviet newspaper, Literaturnaya Gazeta **(Qiu, 2017)**[23]. Dissemination of Soviet propaganda followed a particular pattern wherein, in the first instance, that is the catalyst of the story would be published in a country that is located outside the Soviet Union. In the proceeding steps, it would be picked up by Soviet news agencies adding their own twist to it **(Grimes, 2017)**[24]. The disinformation campaign persisted in the United States for a very long time. In 2005 in a survey, it was clear that a significant proportion of African Americans believed that the U.S. government created the HIV Virus to wipe out the minority communities **(Fears, 2005)**[25].

[22] https://www.globalsecurity.org/intell/library/reports/1987/soviet-influence-activities-1987.pdf - A Report on Active Measures and Propaganda, 1986 – 87
[23] https://www.nytimes.com/2017/12/12/us/politics/russian-disinformation-aids-fake-news.html - Fingerprints of Russian Disinformation: From AIDS to Fake News
[24] https://www.theguardian.com/science/blog/2017/jun/14/russian-fake-news-is-not-new-soviet-aids-propaganda-cost-countless-lives
[25] https://www.washingtonpost.com/wp-dyn/articles/A33695-2005Jan24.html?itid=lk_inline_manual_10

Modern-day disinformation campaigns have become easier to disseminate to the unassuming public citizen. Social media is increasingly becoming securitized by both state and non-state actors. Concerning state actors, authoritarian regimes sow division through the use of systematic information campaigns. Manipulation of public opinion over social media is a danger to public life at a time when the consumption of news is increasingly becoming digital. Although the internet has expedited avenues for civic participation in democratic electoral processes – the significant rise of technology which brings forth instruments such as big data analytics, and computational propaganda has become a major point of concern for policymakers around the world **(Bradshaw, Howard, 2018)**[26].

Both China and Russia have exploited this chasm by learning how to reach wider audiences online thereby leading to a higher level of mass manipulation. Malicious actors and state propagandists have made the most out of the weaponization of information on an unprecedented scale. These actors make the most out of computational propaganda, state-sponsored sock-puppet networks and troll armies **(Posetti, Matthews, 2018)**[27]. With the intensification of research in the domain of Artificial Intelligence (AI), the field of unsupervised learning through the means of generative adversarial networks can easily automate and conceptualize fakes. Both China and Russia have been hopping on the weaponization of artificial intelligence to

[26] https://demtech.oii.ox.ac.uk/research/posts/challenging-truth-and-trust-a-global-inventory-of-organized-social-media-manipulation/
[27] https://www.icfj.org/news/short-guide-history-fake-news-and-disinformation-new-icfj-learning-module

conceptualize deep learning-enabled deep fakes which can be reached out to larger audiences both domestically and internationally **(Polyakova, 2018)**[28].

A growing number of political entities and governments around the world are employing a mixture of both humans and bots to dictate and take part in political conversations across the broad spectrum of social media. As such bots can perform a wide array of tasks such as conversing with humans to update an order or they can be tools of more malicious intent such as helming copy-pasta campaigns and working sending links with malevolent content **(Howard, Kollanyi, 2016)**. It is unclear to what extent political bots succeed in shaping public opinion, although there is plenty of evidence that they do help in the propagation of fake news. According to research done by Carnegie Mellon University during the COVID-19 pandemic, social media bots account for up to 60 percent of all Twitter activity related to the pandemic. **(Young, 2020)**[29]**.** Bots are run on behalf of real or fake individuals sometimes fully automated or the other times operated in tandem with humans. With the sophistication of technology through the means of natural-language processing capacities, bot detection is becoming harder **(Zaman, 2018; el Hjouji et al., 2018)**[30]**.** The sheer value of computational propaganda made available already through the means of data mining has time and again helped malign elections and spread disinformation at the same time **(Woolley, Howard, 2020)**[31].

[28] https://www.brookings.edu/research/weapons-of-the-weak-russia-and-ai-driven-asymmetric-warfare/
[29] https://www.cmu.edu/news/stories/archives/2020/may/twitter-bot-campaign.html
[30] https://arxiv.org/abs/1810.12398
[31] https://ijoc.org/index.php/ijoc/article/viewFile/6298/1809

3.4 Understanding China–Russia relations

China and Russia have had a long-standing complicated relationship with each other. The vast shared border between the two states, as well as ideological differences, have all caused tensions to flare in the past. Despite not being formal allies, both the countries have expanded trade and defence ties with one another. Their shared desire to curb the sphere of influence of the United States and its allies to create a new era of global order is seen as a common cause for alignment between the two. However, calling China and Russia allies would be far from the truth. It can most certainly be inferred that both nations are strategic partners **(Maizland, 2022)**[32].

It can however be said that the countries' alignment is driven by their common rivalry with the United States and the European Union and in the echoes of establishing a new world order far away from what the West currently panders to. In February 2022, just a few days shy of Russia's invasion of Ukraine, Chinese President Xi Jinping and Russian President Vladimir Putin held talks in Beijing vowing to deepen their strategic cooperation. Despite the talks of deepening ties, China has been put at an awkward position due to Russia's invasion of Ukraine. China has a lot to gain from the ongoing war as it is commonly believed by China watchers that the war has increased the leverage for China by creating a security dilemma in the United States' Russia policy and China Policy, which has in turn intensified the anxiety when it comes to U.S abandonment in the Asia-Pacific region **(Maizland, 2022)** [33].

[32] https://www.cfr.org/backgrounder/china-russia-relationship-xi-putin-taiwan-ukraine
[33] https://www.cfr.org/backgrounder/china-russia-relationship-xi-putin-taiwan-ukraine#chapter-title-0-4

At this point in time however, China is not doing a lot to support Russia apart from rhetorical support, which comes in waves of diplomacy **(Sun, Ivanov, Huang, Repnikova, Wishnick, Chorzempa, 2022)**[34]. The idea of providing military assistance to Russia is futile as well knowing that in doing so, both the US and the European Union (EU) would utilise deterrence such as economic sanctions for instance. At the same time, this enables China to test the boundaries in the information domain as Beijing has time and again enabled a myriad of Russian conspiracy theories regarding biolabs in Ukraine[35] **(Lonas, 2022)**. In a report, Taiwan-based Thinktank Doublethink described this sino–Russian enablement as "one side creates and the other expands, distorting information in a way that is beneficial to both Moscow and Beijing."[36] **(Doublethink Lab, 2022)**

3.5 Social Media as an amplifier of Disinformation

The adaptation of social media as a tool by authoritarian states to disseminate disinformation is not surprising. Social media as a whole act as an important catalyst for the polarization of political discourse. The heavy reliance of firms such as for example Facebook and Twitter on various analytics and metrics, and sensationalism over newsworthiness makes them vulnerable to manipulation by authoritarian states. As such Twitter is a far more powerful conduit utilised by malicious actors to achieve the effective spread of propaganda. According to Jarred Prier, the difference between Facebook and Twitter lies in the fact that "on Facebook, your connections are typically more intimate connections than you would expect on Twitter, which

[34] https://www.chinafile.com/conversation/what-does-putins-invasion-of-ukraine-mean-china-russia-relations
[35] https://thehill.com/policy/international/china/597812-china-backs-unsubstantiated-russian-claims-of-us-biolabs-in/
[36] https://euvsdisinfo.eu/the-nazification-of-ukraine-inthe-chinese-information-space/

focuses less on bringing people together and more on bringing ideas together."[37] **(Jarred Prier, 2021**) One of Prier's key arguments is that the spread of narratives outside a particular social cluster revolves around the manipulation of a particular trend. He further adds that this manipulation revolves around four factors which are It hinges on four factors: (1) a message that fits an existing, even if obscure, narrative; (2) a group of true believers pre-disposed to the message; (3) a relatively small team of agents or cyber warriors; and (4) a network of automated "bot" accounts **(Ibid)**.

According to Postdoctoral Research Fellow at Stanford University, Samantha Bradshaw, Twitter has several "affordances" which allow state actors to carry out information operations. For instance, when it comes to anonymity, Twitter does not require users to sign up with their real names, thereby not requiring verification with regard to the identity of a particular user either. This helps in the prevalence of fake accounts – both automated as well as genuine to run amok and spread disinformation on Twitter. Similarly, Twitter's follow-based function has led to an increase in the creation of "influencer accounts". Influencer accounts push a particular falsehood to a large volume of followers and these accounts help in setting and playing out the dissemination of a myriad of breaking news-related information. These accounts are often created with a major chunk of followers to give them the legitimacy of being an authority in a particular domain **(Bradshaw, 2020)**[38].

[37] Christopher Whyte, A. Trevor Thrall, and Brian M. Mazanec, Information Warfare in The Age of Cyber Conflict, Routledge (2021), Chapters 2, 11, 12.
[38] https://ora.ox.ac.uk/objects/uuid:e75e4796-d614-454b-b2e2-df6b8659e610

Facebook's main function is to bring friends and family together thereby creating an intimate connection as opposed to Twitter which relies more on sharing thoughts and feelings with like-minded people. However, Facebook's advertising tool has been exploited by Russian agents to target American citizens who are most likely to get persuaded relatively easier based on factors such as political leanings and behavioural and personality traits. The advertisements are then targeted towards either fringe right-wing groups such as gun-rights advocates or minority groups such as Black Lives Matter to propagate polarizing and highly political debates. The use of social media by Russian agents during peacetime to influence the outcome of the 2016 U.S. Presidential Elections demonstrates how political communication can be tampered with thereby sowing discontent and discord in a domestic environment **(Bradshaw, 2020)**.

Beijing's influence operation module across social media is a bit different compared to that of Russian information operations. Primarily for Beijing, it is important to "Tell China's Story Well" in the most convincing way possible. The phrase "Tell China's Story Well" comes from President Xi Jinping's foreign propaganda offensive to boost China's image by telling positive stories about the mainland **(Dwork, 2022)**[39]. Much of China's influence operations are overt. Meaning, that they supplement their narratives by utilising methodologies such as "Wolf Warrior Diplomacy" on Twitter primarily which in itself is explainable by pointing towards CCP-led accounts of diplomats who tweet in coordination by stating the rhetoric that China is not a rogue operator, that China wants to make sure that it is seen as superior when compared

[39] https://www.ie.edu/insights/articles/telling-china-stories-well/

with democratic powers around the world **(Solon, Dilanian, 2020)**[40]. More on China's influence operation will be elaborated upon in the case studies section of this thesis.

The dissemination of disinformation is not limited to either Facebook or Twitter for that matter. Instant messaging services, such as Telegram are becoming key amplifiers of state-affiliated disinformation. During the ongoing Russian invasion of Ukraine, hyperlocal Russian Telegram channels such as Donbass Insider and Bellum Acta, channels with a history of advancing pro-Russian propaganda have been taking the reins of Kremlin-enabled disinformation into their own hands. Most of these channels are custom fit with rhetoric to resonate with towns spread across the length and breadth of the most conflicted regions of Ukraine. The director of the Defending Democratic Institutions project at the Center for Strategic and International Studies, Suzanne Spaulding, calls these Telegram channels "affinity groups" as they target specific narratives to specific populations given the context and scenario **(Smalley, 2022)**[41].

[40] https://www.nbcnews.com/business/business-news/china-s-influence-operations-offer-glimpse-future-information-warfare-n1244065
[41] https://www.cyberscoop.com/network-telegram-russian-disinformation-ukraine-detector-media/

4 Russia's Information Operations Ecosystem

When it comes to the analysis of Russia's disinformation and propaganda ecosystem, multiple terms and concepts have been utilized to describe this particular type of threat. Russia uses the term "information confrontation" to describe this threat in both strategic and military circles. The applicability of this nature of confrontation implies the applicability of using information as a weapon in both peacetimes as well as conflict. Today's Russian information operations infrastructure relies on tools of trade from the nascent days of the Soviet Union. Former NATO spokesperson, Ben Nimmo describes the tactics utilized by Russia as dismissing the critic, distorting the facts, distracting from the main issue and dismaying the audience[42] **(Lucas, Nimmo, 2016)**.

The long-standing usage of Russian political warfare that utilizes disinformation and propaganda as a core tool is known as "active measures" **(GEC, 2020)**[43]. According to retired KGB General Oleg Kalugin, active measures are designed, "to drive wedges in the Western community alliances of all sorts, particularly NATO, to sow discord among allies, to weaken the United States in the eyes of the people in Europe, Asia, Africa, Latin America, and thus to prepare the ground in case the war really occurs." **(Prier, 2021)** [44]

[42] Edward Lucas and Ben Nimmo, "Information Warfare: What Is It and How to Win It," CEPA, November 2015, accessed June 25, 2016.
[43] https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf
[44] Christopher Whyte, A. Trevor Thrall, and Brian M. Mazanec, Information Warfare in The Age of Cyber Conflict, Routledge (2021), Chapters 2, 11, 12.

Modern Russian information operations are derived from *spetspropaganda,* a subject taught by the Russian Military Institute of Foreign Languages in 1942, as well as *agitprop* which can be described as the combination of agitation and propaganda. These techniques didn't naturally dissipate as claimed by the West, more so, these techniques were refurbished and integrated from the Soviet system, into the Russian one **(Lucas, Pomerantsev, 2016)**.

Kremlin propaganda in today's day and age doesn't focus on the left-wing, anti-colonial and labour-led rhetoric it used to during the Cold War, instead, Russian propaganda now supports narratives from both the far-left, as well as far-right movements. Not only does Kremlin-led propaganda try to wedge a barrier between the two, but also promotes the idea that Western liberal-led democracy is a sham **(Ibid)**. Soviet-born British journalist, Peter Pomerantsev, further argues that modern Russian propaganda is enjoyable. He says so by claiming that the Cold War era-led disinformation operations by the Kremlin were dull and boring. Meanwhile, today's disinformation operations are engaging, they combine high-value production. It's just not about the production, today's disinformation operations also evoke a strong sense of nationalistic pride as well as reminiscence **(Ibid)**.

The role of this section is to explain to the reader the pillars of the Kremlin-led machinery of information operations. Thereby this section will go deeper into Russia's media and social media landscape and seeks to answer broader questions about Russia's activities in the contemporary era.

4.1 Organizational Structure

Russia's Disinformation Machine is not strictly limited to one source.

The Kremlin, therefore, makes use of a myriad of sources of disinformation that seek to erode trust and confidence in the Western approach toward democracy. In a special report titled "Russia's Pillars of Disinformation and Propaganda," the U.S. Department of State's Global Engagement Center (GEC) revealed the Russian disinformation ecosystem at play. One interesting observation from the GEC is the fact that not only each individual segment of Russia's Disinformation Machine plays a distinct role, but also, they tend to feed off of one another thereby bolstering and amplifying information operations to a greater audience (**GEC, 2020)**[45].

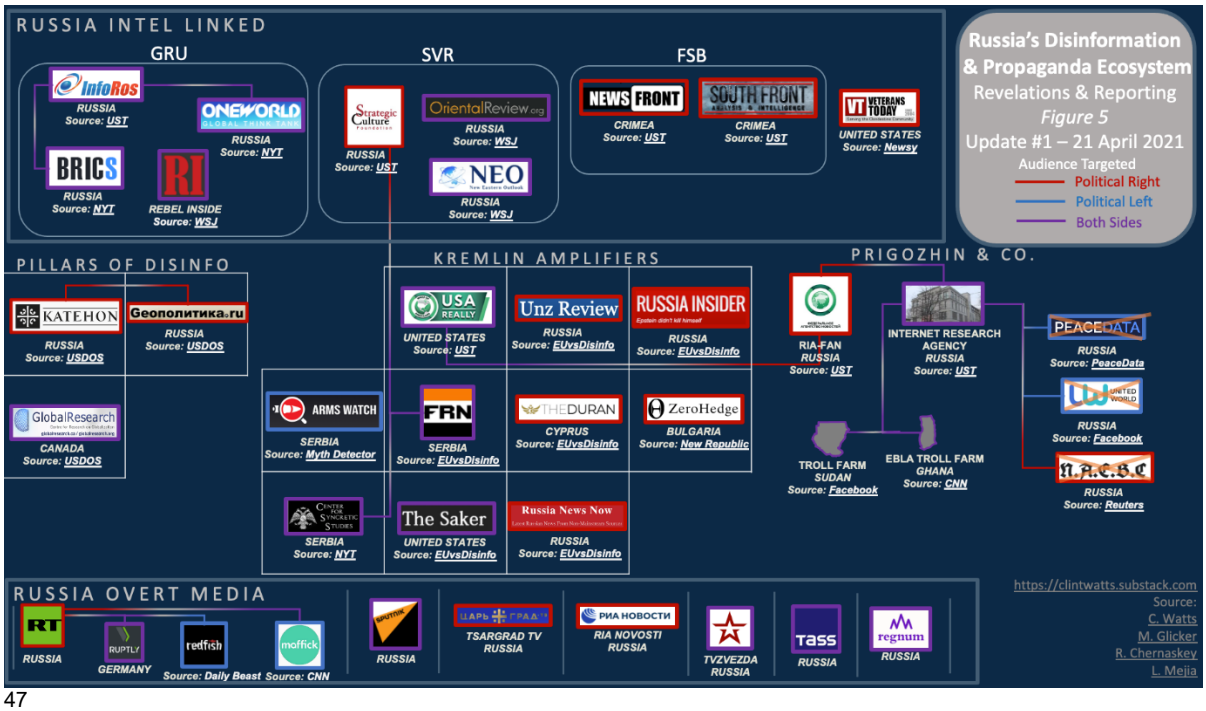
To make it easier to explain the state of play when it comes to Russia's Information Operations Ecosystem, this section will be referring to a diagram visualized by senior fellow at the Center for Cyber and Homeland Security at George Washington University, Clint Watts. Watts has categorized the range and type of Russian outlets as follows **(Clint et al., 2021)**[46]:

- Russian Overt Media: Openly state-sponsored outlets
- Russian Intelligence Linked: Websites with connections to Russian foreign (SVR), domestic (FSB) or military (GRU) Intelligence
- Pillars of Disinformation & Propaganda: Outlets discussed in the Department of State report from August 2020
    - Official Government Communications
    - State-Funded Global Messaging

[45] https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf
[46] https://clintwatts.substack.com/p/russias-disinformation-ecosystem

- Cultivation of Proxy Sources
- Weaponization of Social Media
- Cyber-Enabled Disinformation

- Amplifiers: Websites consistently amplifying pro-Kremlin narratives and discussed in a range of reports from fact-checking outlets and public reporting
- Prigozhin & Co.: Part of the network associated with sanctioned Russian oligarch and owner of the notorious Internet Research Agency (IRA), Yevgeniy Prigozhin



47

The remit of this thesis is not to look at all the categories one by one, the remit of this thesis is therefore only to look at the categories that affect Russia's Information Operations on social media.

[47] Ibid.

4.2 Russia's Overt Influence Capabilities (White)

During the Soviet era, the Central Committee of the Communist Party of the Soviet Union (CPSU) led "white" or overt active measures. The idea of using overt measures during that era was to utilize Russian state-sponsored media outlets. Back then the CPSU was reliant on existing machinery of informational efforts such as TASS, Novosti Press Agency, Radio Moscow, Radio Peace and Progress and other media channels **(Abrams, 2016)**[48].

In the contemporary era, the Kremlin brings to life its Soviet past by using Kremlin-approved English-language news on television as well as on the internet. RT formerly known as Russia Today or Rossiya Segodnya along with Sputnik formerly known as Voice of Russia and RIA Novosti are Russia's primary media outlets that are known for producing content for non-Russian speaking audiences around the world. Unlike more state-affiliated media such as Gazeta.ru or Pravda.ru, the role of RT and Sputnik equate themselves with major independent and international media outlets to increase their credibility. The advantage of Russia's "white" influence capabilities helps in attribution when it comes to global issues that are essential to keep a track of by the Kremlin. RT's leadership consists of the general director, Margarita Simonyan. Simonyan is time and again also referred to as Sputnik's Editor-in-Chief **(GEC, 2022)**[49].

[48] Abrams, Steve. "Beyond Propaganda: Soviet Active Measures in Putin's Russia." *Connections*, vol. 15, no. 1, 2016, pp. 5–31. *JSTOR*, http://www.jstor.org/stable/26326426. Accessed 1 Aug. 2022.

[49] https://www.state.gov/wp-content/uploads/2022/01/Kremlin-Funded-Media_January_update-19.pdf

An interesting case study of disinformation undertaken by Russian state-affiliated media can be attributed to the Liza case in Germany. The central narrative, in this case, was this fake story about a 13-year-old Russian-German girl named Liza, who was purportedly abducted and raped by Arab migrants. Russian state media, exceptionally sensationalized the falsehood and accused the German police of ignoring the incident, thereby refusing to pursue substantial leads on the alleged suspects **(Meister, 2016)**[50]. Despite clarification from the Berlin police that "there was neither an abduction nor a rape", Russian-language media kept promoting the falsehood which led to hundreds of anti-migrant activists protesting on the streets of Germany **(Nimmo, Aleksejeva, 2017)**[51].

4.3 Russia's Semi-Covert Influence Capabilities (Gray)

The idea of a "gray zone" has been around since the Cold War. This particular phenomenon can be described as activities that occur between peace or cooperation and war or armed conflict. A myriad of activities can be inferred in the "gray zone" activities, for instance, cyberattacks, disinformation campaigns and influence operations.

During the Cold War, the Soviet Union was seen as a master of the gray zone domain. The advent of new technologies has provided authoritarian states to engage in these measures using tools that are hard to categorize, attribute or detect which makes it difficult for adversaries to respond in time. Incidentally, it is far easier for authoritarian states to weaponize gray zone-based narrative due to their centralized

[50] https://www.nato.int/docu/review/articles/2016/07/25/the-lisa-case-germany-as-a-target-of-russian-disinformation/index.html
[51] https://medium.com/@DFRLab/lisa-2-0-133d44e8acc7

systems which allows them to utilize a wide array of state-based resources to execute certain operations which wouldn't be possible in democracies due to decentralization **(Starling, Iyer, Giesler, 2022)**[52].

Russian information operations utilize a hub of so-called useful idiots by weaponizing conspiracy theory-oriented websites. The task of these useful idiots is to regurgitate pro-Kremlin narratives without taking direct commands from Russian personnel. The Kremlin uses conspiracy theory-oriented websites such as Info Wars and Zero Hedge to shape themes into strong narratives and disseminate them into hate-mongering groups such as white nationalists. **(Watts, Weisburd, Berger, 2022)**[53].

Covert operations in countries that have had a territorial dispute with Russia such as both Georgia and Ukraine are seen as strong examples of Gray Zone activities as initiated by the Kremlin. In the 21st century Russia has advanced cyberwar capabilities. Russia has time and again utilized these activities to undermine military and civilian economic infrastructures of these nations thereby incapacitating their ability to respond to operations of these kinds. For example, in 2008, the Kremlin waged an offensive cyber campaign against Georgia which inflicted significant damage to the Georgian media infrastructure. In the Ukrainian context, most cyber warfare perpetrated by Russia can be seen in the context of the consequences of a direct military confrontation **(Clingendael, 2021)**.

[52] https://www.atlanticcouncil.org/blogs/new-atlanticist/todays-wars-are-fought-in-the-gray-zone-heres-everything-you-need-to-know-about-it/#what
[53] https://warontherocks.com/2016/11/trolling-for-trump-how-russia-is-trying-to-destroy-our-democracy/

Russian gray zone activities have been under tremendous scrutiny by both academics and policymakers. Calling Russian actions ambiguous helps the Kremlin get ahead of tis Western counterparts as it shows a lack of clear determination by the West to stop the Russian leadership from taking imminent action. Ambiguity was seen as a core of Russian warfare before the full-scale invasion of Ukraine in 2022 **(Jonsson, 2022)**[54].

4.4 Russia's Covert Influence Capabilities (Black)

A 1992 United States Information Agency (USIA) report defined "Black" or covert active measures as follows "… the use of agents of influence, forgeries, covert media placements and controlled media to covertly introduce carefully crafted arguments, information, disinformation, and slogans into the discourse in government, media, religious, business, economic, and public arenas in targeted countries." The KGB's First Chief Directorate, responsible for foreign intelligence operations coordinated the covert active measures operations. The idea was to conceal any kind of attribution of the Soviet role. The KGB's methodology was to act as an agent of influence by weaponizing covert placements across mainstream media outlets, and to introduce pro-Russian arguments, information, disinformation, and slogans in the political discourse of targeted countries **(USIA, 1992)**[55].

After the dissolution of the USSR and therefore by default, the KGB, contemporary era Russian intelligence services such as the Main Directorate of the General Staff

[54] https://www.chathamhouse.org/2022/06/myths-and-misconceptions-around-russian-military-intent/myth-1-russia-waging-grey-zone
[55] http://intellit.muskingum.edu/russia_folder/pcw_era/index.htm

of the Armed Forces of the Russian Federation (GRU), Foreign Intelligence Service (SVR) and the Federal Security Service of the Russian Federation (FSB) took over the reins of covert active measures. In Russia, there is a vast black market of nationalist and/or criminal hacking communities regularly employed by the Kremlin itself in order to carry out cyberattacks on adversarial countries. These hacking communities work on a "pro bono" basis, in the event that the Russian authorities will condone their criminal activities. This particular collaborationist approach helps the Kremlin evade risks of attribution **(Gvosdev, 2012)**[56]. The aforementioned Russian secret and intelligence services operate under sophisticated hacktivist or patriotic hacker groups engaging in activities such as running Distributed Denial-of-Service (DDoS) Attacks, phishing and website compromise **(Greenberg, 2019)**[57]. Russian cyber espionage group, APT28, commonly known as Fancy Bear hacked into the emails of the Democratic National Committee (DNC) and the political party of French President Emmanuel Macron. After extracting the emails, these APTs wait for the opportune moment to dump the content thereby influencing the outcome of a particular election **(Greeberg, 2017)**[58].

The infamous troll farm known as the Internet Research Agency (IRA) has its origins as part of Russia's covert influence capabilities. It is alleged that the was controlled by Russian oligarch and close confidant of Russian President Vladimir Putin, Yevgeny Prigozhin. The IRA is accused by multiple governments such as the US

[56] Nikolas K. Gvosdev. 2012. "Chapter 11: The Bear Goes Digital, Russia and Its Cyber Capabilities" In Reveron, Derek S. *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*. Georgetown University Press

[57] Greenberg, Andy. 2019. "A Brief History of Russian Hackers' Evolving False Flags" in *Wired*. https://www.wired.com/story/russian-hackers-false-flags-iran-fancy-bear/

[58] https://www.wired.com/2017/05/russian-hackers-using-tainted-leaks-sow-disinformation/

and the UK for example of using a troll factory to spread disinformation on social media **(UK GOV, 2022)**[59]. More about the role of the IRA and its past will be uncovered in the analysis section of this dissertation.

5 China's Propaganda Ecosystem

In a lengthy commentary published in Qiushi, the Chinese Communist Party's theoretical and ideological journal, the deputy director of the Propaganda Department, Zhuang Rongwen (庄荣文), remarked that "the internet is one network, and online propaganda and public opinion work is one chessboard" **(Creemers, Triolo, Webster, 2018)**[60].

China's propaganda efforts are diverse when compared to Russia. Russia's information operations are primarily focused on the cyber domain as evidenced by the use of hacktivists and the constant interference in influencing democratic elections in the West. Meanwhile, China's information operations are more categorized on economic, political, and personal relationship-building globally. Under President Xi Jingping, China wishes to reshape the current international system in the way it sees fit, thereby challenging the United State's status as the world's only hegemon **(Recorded Future, 2019)**.

The idea of utilizing information influence operations as a tool of cyberwarfare arrived well before the discovery of the internet itself. Chairman of the Communist Party of China, Mao Zedong embraced propaganda which was drawn from the likes

[59] https://www.gov.uk/government/news/uk-exposes-sick-russian-troll-factory-plaguing-social-media-with-kremlin-propaganda

[60] https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-new-top-internet-official-lays-out-agenda-for-party-control-online/ - Translation: China's new top Internet official lays out agenda for Party control online

of the Soviets **(Shambaugh, 2007)**.[61] In doing so, Zedong exploited foreign contacts right from the very beginning to shape the story of China's revolution by discrediting its adversaries. For instance, between the 1930s to the 1940s, Mao conspired with the Japanese army to wear down the Kuomintang (KMT) forces led by Chiang Kai-shek **(Homare, 2016)** [62]. Other examples of the CCP's deep reservoir of experience can be attributed to the Korean War of 1952 wherein Chinese information operations worked relentlessly to spread the falsehood that germ warfare was waged by the United States, which was responsible for the outbreak of diseases such as Cholera, bubonic plague etc in China and North Korea **(Chen, 2009)** [63]. The CCP back then combined the art of overt and covert propaganda by spreading this falsehood across the length and the breadth of Chinese propaganda outlets. Despite the outright rejection from the U.S, journalists such as John Powell declared that the United States "surpasses the savagery of Hitler Germany and Hirohito Japan" and "shocked and horrified the entire world" **(Ibid)** [64].

When it comes to the fabrication of propaganda, the CCP has had a large bureaucratic structure for information control. The ideological effort laid down by the party is on two levels: the first one is to shape its own internal politics thereby maintaining the party's legitimacy and the second one is to influence international opinion by waging "information war" in favor of Chinese interests **(Jeangène Vilmer,**

[61] Shambaugh, David (January 2007). "China's Propaganda System: Institutions, Processes and Efficacy". China Journal. 57 (57): 25–58. doi:10.1086/tcj.57.20066240. JSTOR 20066240. S2CID 140932475.
[62] https://u.osu.edu/mclc/2016/07/02/truth-of-mao-zedongs-collusion-with-the-japanese-army-1/
[63] Shiwei Chen, "History of Three Mobilizations: A Reexamination of the Chinese Biological Warfare Allegations against the United States in the Korean War," The Journal of American-East Asian Relations 16, no. 3 (2009): 225-226.
[64] Ibid

Escorcia, Guillaume, Herrera, 2018)[65]. In the contemporary era, the CCP has built sprawling infrastructure for manipulating information. It seeks to promote various ideals such as the intellectual debate on China when it comes to a peaceful rise and harmonious society. The theory of peaceful rise refers to the construction of this image that the theory of "Chinese threat" doesn't exist, and that China's international footprint will be consolidated by China's harmless and pacifist nature **(Jeangène Vilmer**, **Charon, 2022)[66].**

The dissemination of Chinese propaganda has gained a major foothold both at home and abroad through the longstanding capabilities of emerging technologies. It is all too obvious that an inevitable comparison with the Russian methodology of expansion of influence operation was always on the cards. China's experience in the field of sophisticated propaganda has been largely amplified due to the internet. The CCP has time and again integrated newer forms of technologies in a structure that is unlike any other in the world.

5.2 Organizational Structure

Chinese influence operations are partly enthused by their Soviet counterparts. The role of this section will be to explore two major doctrinal resources. The first one is the three-warfares doctrine [三战]. The three warfares doctrine, encompasses psychological warfare (心理战), public opinion warfare (舆论战), and legal warfare (法律战). The PLA adopted this doctrine after the 2003 U.S. Invasion of Iraq as it

[65] https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf
[66] https://www.irsem.fr/report.html

was inspired by the total domination of the U.S. in the digital battlespace. Even though the three-warfares doctrine has a military-based connotation it has frequently been utilized beyond the outreach of the military domain. The second doctrinal resource refers to the United Front (统一战线), which itself is managed by the CCP's United Front Work Department (UFWD) **(Ibid)**. Chairman Mao listed the United Front among the "three magic weapons" that helped bring him to power **(Brady, 2017; Li-hua, Chung, 2019)**[67].

5.2.1 The United Front (统一战线)

At the 2015 Central United Front Work Meeting, Chinese President Xi Jinping echoed in Chairman Mao's footsteps by stating that 'the United Front … is an important magic weapon for strengthening the party's ruling position … and an important magic weapon for realizing the China Dream of the Great Rejuvenation of the Chinese Nation' **(Lunde, 2015)[68].** Since the 18th National Congress of the Communist Party of China, Xi Jinping's series of expositions on the status and role of the united front have pushed the party's united front work into a new era and created a lively and lively way for all classes to participate in political life and major national decision-making in an orderly manner **(Ibid)**. The United Front maintains a complex and impervious set of establishments designed to advance the CCP's influence

[67] Anne-Marie Brady, Magic Weapons: China's Political Influence Activities under Xi Jinping, Wilson Center, September 18, 2017, https://www.wilsoncenter.org/article/magic-weapons-chinas-political-influenceactivities-under-xi-jinping; Chung Li-hua and Jake Chung, "China Using Local 'Agents' to Spread Misinformation Online: Institute," Taipei Times, August 4, 2019, http://www.taipeitimes.com/News/front/archives/2019/08/04/2003719873.

[68] https://web.archive.org/web/20190826053157/http:/www.tibet.cn/cn/news/yc/201712/t20171222_5282108.html

operations both domestically and internationally. By doing so, the United Front engages in overt and clandestine activities including cultural exchanges, supporting criminal gangs like the Triads, and civic associations **(Diresta, Miller, Molter, Pomfret, Tiffert, 2020)**[69].

Since the United Front prefers to operate with a greater degree of plausible deniability, by co-opting pro-Chinese interest groups. For instance, in the U.K. and the U.S., the CCP engages in political activity by promoting student and scholar organizations, in order to pressurize university administrators to cancel visits from the Dalai Lama for example or to funnel counter-protests against criticism of the CCP's actions in Xinjiang **(Fedasiuk, 2022)**[70]. Researchers from the Center for Security and Emerging Technology (CSET) have identified 'science and technology diplomats' (科技外交官) – staff allocated to the science and technology directorates across Chinese embassies and consulates who work on identifying technology-oriented projects of strategic consequence to the CCP **(Fedasiuk, Weinstein, Puglisi, 2021)**[71].

5.2.2 The Three Warfares Doctrine (三战)

When it comes to gauging success, today's legislators as well as armed forces are faced with a dilemma. Harvard Professor John Nye has described this dilemma through the lens of twenty-first-century conflicts. Professor Nye remarks that conflicts in the contemporary era are more about whose story wins, as opposed to whose

[69] https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/sio-china_story_white_paper-final.pdf
[70] https://www.aspistrategist.org.au/how-chinas-united-front-system-works-overseas/
[71] https://cset.georgetown.edu/publication/chinas-foreign-technology-wish-list/

army **(Jackson, 2015)**[72]. The three-pronged strategy representing most of the Chinese political warfare is one of the main doctrines of the People's Liberation Army (PLA). Chinese scholars understand the three warfares doctrine to be a form of non-kinetic conflict. The logic behind it comes from the idea that waging political warfare symbolizes winning without fighting. For International Relations (IR) scholars, the three warfares doctrine is a contested form of warfare as it can also be considered to be a form of hybrid warfare that blurs the boundary between war and peace, combatant and civilians and of course military and non-military methodology **(Jeangène Vilmer**, **Charon, 2022)**[73]. Many scholars might also argue that the Three Warfares is an extension of information warfare. Chinese military writings have showcased the extent to which achieving information superiority is seen as a pivotal aspect to achieve battlefield supremacy **(Singh, 2013)**[74].

5.2.3 Psychological Warfare

Psychological warfare is widely acknowledged to be one of the most important aspects of the Three Warfares. The ability to demoralize and destroy enemy forces makes them question their own tenacity. Psychological Warfare during peacetime works on influencing and altering a person's implicit views to make them more susceptible to intimidation. The PLA's way of psychological warfare is further divided into four different types; Coercion (威慑), which aims to persuade someone else to behave in a certain way, Mystification (欺诈) confuses and leads to deception and

[72] https://li.com/reports/information-at-war-from-chinas-three-warfares-to-natos-narratives/
[73] https://www.irsem.fr/report.html
[74] https://idsa.in/system/files/jds_7_4_AbhijitSingh.pdf

"division" (离间) which seeks to undermine the motivation of the adversary by taking advantage of any potential flaws and conflicts and paralyses its decision-making process. Lastly, Defense (防护), is used to preserve the morale of one's own troops when they are the focus of analogous hostile efforts. 28 **(Jeangène Vilmer**, **Charon, 2022)**[75].

China uses psychological warfare on both domestic, as well as foreign-based adversaries. A prime example of China carrying out psychological warfare on the domestic populous can be attributed to the Chinese regime's actions against the Uyghur ethnic minority. The Uyghurs are a majority-Muslim Turkic ethnic group that has been violently repressed over the past few decades or so. In doing so the Chinese regime utilizes a bunch of methodologies such as random detainments, large-scale internments, digital surveillance, and regular inspections among other forms of psychological warfare **(Jeangène Vilmer**, **Charon, 2022)**[76].

When it comes to an example of China using psychological warfare on a foreign-based adversary, an important example to bring to light is China's relationship with India. Since 2010, the PLA has enhanced its military posture in Tibet. Improving military-based infrastructure, and undertaking training for high-altitude mountain warfare are all reaching points of equilibrium with what can be called the militarization of Tibet. The rapidity through which the PLA is constructing infrastructure along the Sino-Indian borders is a cause for concern in the eyes of the Indian Army. However, most scholars would agree that this constitutes a form of a psychological warfare tactic by using coercion **(Singh, 2013)**.

[75] https://www.irsem.fr/report.html
[76] https://www.irsem.fr/report.html

5.2.4 Public Opinion Warfare (also known as Media Warfare)

The primary goal of public opinion warfare, also known as media warfare on a broader level is to win over target audiences. Public opinion warfare, as conceptualized by the Chinese, consists in carrying out the "cognitive orientation" (引导认知) of the masses, to excite their emotions (激发情感) and to constrain their behavior (约束行为). This form of warfare involves the use of all forms of media such as the press, radio, television, social networks in China (WeChat, Weibo, TikTok) as well as social media outside China (Facebook, YouTube, Twitter) films, and books as tools of influence **(Jeangène Vilmer**, **Charon, 2022)**[77]. For the PLA, the formulation of this form of warfare was inevitable as it had first had witnessed the role of the internet in military operations through the NATO campaign against Muammar Gaddafi in Libya in 2011. In September 2015, in an article the PLA Daily asserted that "from Libya to Iraq, from Ukraine to Syria, social networks have already become a new battlefield that all parties in a conflict intensely engage" **(Beauchamp-Mustafaga, Chase, 2019)**[78]. President Xi's vision of "telling China's story well" is an important part and parcel that paves way for this particular doctrine to succeed on social media. The PRC state media has time and again invested in its overseas operations via Chinese state-affiliated media channels such as Xinhua, China's official state news agency and the China Global Television Network (CGTN), that has numerous foreign bureaus and broadcasts in several languages **(Diresta, Miller, Molter, Pomfret, Tiffert, 2020)**.

[77] https://www.irsem.fr/report.html
[78] https://www.fpi.sais-jhu.edu/_files/ugd/b976eb_ad85a42f248a48c7b0cb2906f6398e71.pdf

One of the most observable overt forms of public opinion warfare can be accredited to China's Wolf Warrior Diplomacy (战狼外交) wherein PRC diplomats actively promote and defend China's interests and image abroad throughout various media platforms. These wolf warrior diplomats were primarily active during the Covid-19 pandemic to respond to particular criticisms levelled against China, most of which stemmed from China's inefficient management of the virus within China, as well as Beijing's responsibility in hiding the flow of information from other countries **(Jeangène Vilmer**, **Charon, 2022)**[79]. Several Chinese diplomats and embassies have had an active presence on Twitter since 2019. Few of them have amassed a massive following for their no-nonsense approach in rebutting accusations levied against China. As of writing the Deputy Director of the Foreign Ministry Information Department of China, Zhao Lijian has close to 1.5 million followers[80] and similarly the Assistant Minister of Foreign Affairs of the People's Republic of China, Hua Chunying has a following of close to 1.4 million followers[81].

5.2.5 Legal Warfare

When it comes to legal warfare, Beijing uses this medium to exploit legal system both domestically and internationally in order to drive political as well as commercial games through this medium. Chinese scholars have defined legal warfare as the use of law as a weapon of war to acquire normative superiority, therefore justifying the Chinese plan of action if it comes to using force to during a conflict for example. Out of all three mediums under the Three Warfares doctrine, legal warfare fulfills the

[79] https://www.irsem.fr/report.html
[80] https://twitter.com/zlj517
[81] https://twitter.com/SpokespersonCHN

dream of Chinese revisionism. As noted in the introduction part of this dissertation, China has time and again utilized legal warfare in the conflicted South China Sea to trespass maritime laws and boundaries in order to serve its interest **(Jackson, 2015)**[82].

China has time and again manipulated the law of the sea duly formulated by the United Nations Convention on the Law of the Sea (UNCLOS) in 1982 to establish a stronger foothold in the South China Sea. The CCP refuses to recognize mandates issued by the Permanent Court of Arbitration of The Hague which in 2016 stated that the Chinese territorial claim of the "Nine-Dash Line" had no legal basis. Despite that China maintains strong navy presence in the disputed territory. With this particular module of the doctrine, Beijing wants the world to play by its rules **(Jeangène Vilmer**, **Charon, 2022)**[83]. A contentious example of China using this module in a domestic setting can be referred to the June 30, 2020 Hong Kong national security law passed by Beijing. Upon passing the extraterritoriality of Article 38, anyone that criticizes the CCP can now be pursued and arrested if they travel to Hong Kong, China, or even third-party countries that allow Chinese authorities to act on their soil **(Ibid)**.

6 Case Study 1: Russian Information Operations in Ukraine

6.1.1 Background

One cannot study modern Russian Information Operations without covering Ukraine. The Kremlin's strategic approach since 2014 in Ukraine relies heavily on Russia's

[82] https://li.com/reports/information-at-war-from-chinas-three-warfares-to-natos-narratives/
[83] https://www.irsem.fr/report.html

concept of information warfare. Russia's version of information warfare is not defined in the same way as the West thinks about the concept. Instead, Russia's methodology relies extensively on hybrid warfare which entails the use of deliberate disinformation campaigns as supported by various Russian based intelligence organizations such as the SVR, FSB and the GRU. Disinformation helps conceal the Russia's objectives. Full-fledged Russian military reforms started during the 2008 Russo-Georgian War when the Russian forces suffered from the outdated Soviet weaponry while fighting Georgians who were equipped by the West. These technological deficiencies paved the way for the improvisation of the command-and-control structures thereby focusing more on shrinking the size of the army by being efficient and mobile. **(Snegovaya, 2015)[84].**

The appointment of Valery Gerasimov in 2012 paved the way for a greater impetus to be put on information operations. Gerasimov was instrumental in conceptualizing the Gerasimov doctrine in which he took tactics ideated upon by the Soviet Union, blended them into cacophonies of total war with strategic military thinking and laid out a doctrine that focuses on modern warfare above all **(McKew, 2017)[85]**. Prior Russian doctrines of total war were on the expensive side, the Gerasimov doctrine was cost-efficient and stressed on more hybrid forms of warfare. At some point of time the Kremlin did understand its position of military weakness against a powerful NATO, thereby choosing to focus on the aspects that the Russian intelligence community succeeded in more **(Snegovaya, 2015)[86].** Gerasimov stressed on the

[84] https://www.understandingwar.org/report/putins-information-warfare-ukraine-soviet-origins-russias-hybrid-warfare
[85] https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia-foreign-policy-215538/
[86] https://www.understandingwar.org/report/putins-information-warfare-ukraine-soviet-origins-russias-hybrid-warfare

idea that the information space opens up a dynamic range of possibilities to reduce the fighting potential of the enemy **(Ibid)**.

6.1.2 Analysis

Since 2014, the Gerasimov Doctrine has been deployed in Ukraine to substantial effect. In the very same year, quite a lot of events took place which led to the cognitive dissonance of the Ukrainians. For instance, in February 2014, the Maidan Revolution took place in the country. The goals of the Maidan Revolution from the Ukrainian side was the removal of then President Viktor Yanukovych which culminated from the sudden decision of Yankovich to foster closer ties to Russia and the Eurasian Economic Union as compared with the European Union. During this time, the Kremlin chose to deploy the Gerasimov Doctrine by supporting both the pro-Russian forces and Ukrainian ultra-nationalists which the Kremlin eventually used as a ploy to seize Crimea and launch war in the Eastern parts of Ukraine **(McKew, 2017)**[87].

With the advancement in technology, traditional forms of Russian media extended themselves into newer communications platforms. Media outlets such as RT and Sputnik heralded in a global audience after these media outlets started regurgitating content in the English language. Ever since the beginning of the Crimean crisis, the Kremlin's traditional media set forth the agenda of putting Ukraine in a negative picture **(Jaitner, Mattsson, 2015)**[88].

[87] https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia-foreign-policy-215538/
[88] https://ccdcoe.org/uploads/2018/10/Art-03-Russian-Information-Warfare-of-2014.pdf

It is truly an intriguing state of affair as Russia utilizes the same narratives from 2014 in its 2022 invasion of Ukraine. For instance, Moscow propagandists focused on head of the Organization of Ukrainian Nationalists and Nazi Collaborator, Stepan Bandera. Russia's propaganda machinery drew parallels between Bandera's extermination of the Jews in collaboration with the Nazi regime and the Ukrainian defense forces and its volunteer units **(Sazonov, Müür, 2017)**[89]. Vladimir Putin's speech on the 25th of February, 2022 echoed the Kremlin's long standing information operations with regards to the relation of Ukraine and Stepan Bandera. In the speech Putin addressed his enemies by stating that "do not allow neo-Nazis and Banderites to use your children, your wives and the elderly as a human shield. Take power into your own hands. It seems that it will be easier for us to come to an agreement than with this gang of drug addicts and neo-Nazis" **(Roth, 2022)**[90]**.**

Towards the starting of the year, Russian information operations took shape in the form of cyberattacks. On the 14th of January the websites of several Ukrainian government websites such as the Ministry of Foreign Affairs of Ukraine were defaced with messages in Russian, Ukrainian and Polish claiming that sensitive data was hacked from these government websites and would be released. American cybersecurity firm, Mandiant, attributed this cyberattack to the deployment of destructive tools such as PAYWIPE and SHADYLOOK. Both of which were disguised as malware and file corrupter respectively **(Wahlstrom, Revelli, Riddell, Mainor, Serabian, 2022)**[91]. A similar kind of information operation took place on the 23rd of February, just a few days before the official declaration of a "special

[89] https://www.ksk.edu.ee/wp-content/uploads/2017/11/RUSSIAN-INFORMATION-WARFARE-AGAINST-UKRAINE-koolon-I-ONLINE-NEWS-AND-SOCIAL-MEDIA-ANALYSIS.pdf
[90] https://www.theguardian.com/world/2022/feb/25/its-not-rational-putins-bizarre-speech-wrecks-his-once-pragmatic-image
[91] https://www.mandiant.com/resources/information-operations-surrounding-ukraine

operation" by Vladimir Putin wherein more Ukrainian government websites defaced. The sophistication of Russian information operations kept increasing with the war as in the following month, a "deepfake" video impersonation of Ukrainian President Volodymyr Zelenskyy purportedly surrendering to the Russian forces was debunked and removed on social media **(Evon, 2022)**[92].

7 Case Study 2: Chinese Influence Operations in light of the COVID-19 pandemic

7.1.1 Background

Since the emergence of the Coronavirus disease (COVID-19) and the eventual labelling of the same as a pandemic, various narratives began to surface suggesting that the virus had emerged from the Wuhan Huanan Seafood Wholesale Market located in the Wuhan City, the capital of Hubei Province in Central China. The disease in itself was spreading rapidly without the knowledge of any effective treatment. During the age of social media, China's narrative control featuring both overt and covert mechanisms forms an important study. The CCP's initial steps to make sure that the narrative is controlled was to censor negative cover of the pandemic, especially rhetoric coming from Chinese whistleblowers. Several imperative Chinese journalists and medical personnel were forcibly disappeared by the government when they tried to blow the lid on the CCP trying to cover up the damages **(Diresta, Miller, Molter, Pomfret, Tiffert, 2020)**[93].

[92] https://www.snopes.com/news/2022/03/16/zelenskyy-deepfake-shared/
[93] https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/sio-china_story_white_paper-final.pdf

Chinese state media began an information offensive against its domestic as well as international audiences by conjuring and promoting frugal conspiracy theories. The CCP has tried to deflect the blame for mismanagement to other countries. Prominent influencer, as well as media accounts both on the Chinese internet as well as their Western counterparts began peddling the falsehood that the COVID-19 virus was bioengineered by U.S. military personnel from the military installation in Frederick, Maryland. The complicated history of this particular installation stems from the fact that Fort Detrick currently houses biomedical labs researching viruses such as Ebola and smallpox **(Palmer, 2021)**[94].

7.1.2 Analysis

Controlling the Domestic Narrative

The initial part of damage control of the CCP was to control the internal narratives. By imposing a tight control over social networks as well as traditional media outlets, central authorities tried to silence important whistleblowers, whose profession ranged from doctors to journalists. The Chinese media was instructed by the overarching propaganda machinery to make the China's response to the pandemic as nothing short of heroic. Beijing followed this by suspending journalists from various Western media organizations such as the expulsion of U.S. based journalists from the Wall Street Journal, New York Times etc for allegedly restricting Chinese state media from operating in the United States. Post which the CCP was involved in making

[94] https://foreignpolicy.com/2021/08/11/china-coronavirus-origin-conspiracy-wilson-edwards-fort-detrick/

itself look like victims of a Western information offensive **(Diresta, Miller, Molter, Pomfret, Tiffert, 2020)**[95].

Controlling the International Narrative

The second aspect in Chinese information operations emanating from COVID-19 focused on demonizing voices from the West that levied various forms of criticism on the Chinese government during the initial weeks of the pandemic. The director of the Lau China Institute at King's College London, Kerry Brown, remarked this atrophy by stating that "In this environment in China, there's no punishment for people who are overzealous in defending China. You're not going to lose your job if you overstep. Everyone is trying to demonstrate their loyalty" [96] **(Bengali, Su, 2020)**. China tried to change this particular rhetoric by focusing on and creating an image of benevolent China. To do so, China focused on the construction of a narrative that China, just like the rest of the countries across the world was equally affected by the pandemic and yet willing to help countries in dire need. This particular campaign of positivity was widely disseminated across Europe in countries such as France for instance, the Chinese embassy spread the rhetoric that "China helps European countries" **(Jeangène Vilmer**, **Charon, 2022)**[97]. While these methodologies are overt, China's effort to control the COVID-19 narrative took shape in covert methodologies as well. For instance, a BBC News investigation led by Bellingcat researcher Benjamin Strick found a coordinated inauthentic network of 1,000 Twitter accounts, 53 Facebook pages, 61 Facebook accounts and 187 YouTube channels that promoted the CCP's

[95] https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/sio-china_story_white_paper-final.pdf
[96] https://www.latimes.com/world-nation/story/2020-05-04/wolf-warrior-diplomats-defend-china-handling-coronavirus
[97] https://www.irsem.fr/report.html

narrative based on COVID-19. Eventually these accounts were taken down and flagged as inauthentic behavior infested accounts by the security team at Twitter **(Strick, Robinson, Sadarizadeh, 2020)**[98].

[98] https://www.bbc.com/news/blogs-trending-52657434

10 Bibliography

@DFRLab (2017). *Lisa 2.0*. [online] Medium. Available at: https://medium.com/@DFRLab/lisa-2-0-133d44e8acc7 [Accessed 2 Aug. 2022].

Abrams, S. “Beyond Propaganda: Soviet Active Measures in Putin’s Russia.” Connections, vol. 15, no. 1, 2016, pp. 5–31. JSTOR, http://www.jstor.org/stable/26326426. Accessed 1 Aug. 2022.

August 2020 Pillars of Russia’s Disinformation and Propaganda Ecosystem. (2020). [online] Available at: https://www.state.gov/wp-content/uploads/2020/08/Pillars-of-Russia%E2%80%99s-Disinformation-and-Propaganda-Ecosystem_08-04-20.pdf.

Background to " Assessing Russian Activities and Intentions in Recent U.S. Elections ": The Analytic Process and Cyber Incident Attribution. (2017). [online] Available at: https://www.dni.gov/files/documents/ICA_2017_01.pdf.

Beauchamp-Mustafaga, N. and Chase, M. (n.d.). *Foreign Policy Institute Borrowing a Boat Out to Sea: The Chinese Military’s Use of Social Media for Influence Operations*. [online] Available at: https://www.fpi.sais-jhu.edu/_files/ugd/b976eb_ad85a42f248a48c7b0cb2906f6398e71.pdf [Accessed 2 Aug. 2022].

Bengali, S., Su, A. (2020). *‘Put on a mask and shut up’: China’s new ‘Wolf Warriors’ spread hoaxes and attack a world of critics*. [online] Available at: https://www.latimes.com/world-nation/story/2020-05-04/wolf-warrior-diplomats-defend-china-handling-coronavirus.

Bradshaw, S. (2020). *The social media challenge for democracy: propaganda and disinformation in a platform society*. [online] ora.ox.ac.uk. Available at: https://ora.ox.ac.uk/objects/uuid:e75e4796-d614-454b-b2e2-df6b8659e610 [Accessed 21 Sep. 2021].

Bradshaw, S. and Howard, P. (2010). Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation. *Ox.ac.uk*, [online] 2017.12. Available at: https://ora.ox.ac.uk/objects/uuid:cef7e8d9-27bf-4ea5-9fd6-855209b3e1f6.

Brady, A. Magic Weapons: China’s Political Influence Activities under Xi Jinping, Wilson Center, September 18, 2017, https://www.wilsoncenter.org/article/magic-weapons-chinas-political-influenceactivities-under-xi-jinping;

Brangetto, P. and Veenendaal, M. (2018). *Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations*. [online] Available at: https://ccdcoe.org/uploads/2018/10/Art-08-Influence-Cyber-Operations-The-Use-of-Cyberattacks-in-Support-of-Influence-Operations.pdf.

Chatham House – International Affairs Think Tank. (2022). *Myth 1: 'Russia is waging "grey-zone" warfare'*. [online] Available at: https://www.chathamhouse.org/2022/06/myths-and-misconceptions-around-russian-military-intent/myth-1-russia-waging-grey-zone [Accessed 2 Aug. 2022].

ChinaFile. (2022). *What Does Putin's Invasion of Ukraine Mean for China-Russia Relations?* [online] Available at: https://www.chinafile.com/conversation/what-does-putins-invasion-of-ukraine-mean-china-russia-relations [Accessed 2 Aug. 2022].

Chung, Li and Chung, J, "China Using Local 'Agents' to Spread Misinformation Online: Institute," Taipei Times, August 4, 2019, http://www.taipeitimes.com/News/front/archives/2019/08/04/2003719873

Cohen, J. (2020). *Scientists 'strongly condemn' rumors and conspiracy theories about origin of coronavirus outbreak*. [online] Available at: https://www.science.org/content/article/scientists-strongly-condemn-rumors-and-conspiracy-theories-about-origin-coronavirus.

Cremiers et al. (2018). *Translation: China's new top Internet official lays out agenda for Party control online*. [online] Available at: https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-new-top-internet-official-lays-out-agenda-for-party-control-online/ [Accessed 2 Aug. 2022].

DiResta, R., DiResta, R., Miller, C., Molter, V., Pomfret, J. and Tiffert, G. (2020). Telling China's Story: The Chinese Communist Party's Campaign to Shape Global Narratives. *fsi.stanford.edu*. [online] Available at: https://fsi.stanford.edu/publication/telling-chinas-story [Accessed 20 Dec. 2021].

Dwork, B. (2022). *Telling China Stories Well?* [online] Available at: https://www.ie.edu/insights/articles/telling-china-stories-well/ [Accessed 2 Aug. 2022].

Evon, D. (2022). *Bad Deepfake of Zelenskyy Shared on Ukraine News Site in Reported Hack*. [online] Available at: https://www.snopes.com/news/2022/03/16/zelenskyy-deepfake-shared/ [Accessed 2 Aug. 2022].

Fears, D. (2005). *Study: Many Blacks Cite AIDS Conspiracy (washingtonpost.com)*. [online] Available at: https://www.washingtonpost.com/wp-dyn/articles/A33695-2005Jan24.html?itid=lk_inline_manual_10 [Accessed 2 Aug. 2022].

Fedasiuk, R. et al. (2021). *China's Foreign Technology Wish List*. [online] Available at: https://cset.georgetown.edu/publication/chinas-foreign-technology-wish-list/ [Accessed 2 Aug. 2022].

GOV.UK. (2022). *UK exposes sick Russian troll factory plaguing social media with Kremlin propaganda*. [online] Available at: https://www.gov.uk/government/news/uk-exposes-sick-russian-troll-factory-plaguing-social-media-with-kremlin-propaganda.

Greenberg, A. (2019). *A Brief History of Russian Hackers' Evolving False Flags*. [online] Available at: https://www.wired.com/story/russian-hackers-false-flags-iran-fancy-bear/.

Greenberg, A. (n.d.). *Russian Hackers Are Using 'Tainted' Leaks to Sow Disinformation*. [online] Wired. Available at: https://www.wired.com/2017/05/russian-hackers-using-tainted-leaks-sow-disinformation/ [Accessed 2 Aug. 2022].

Grimes, D. (2017). *Russian fake news is not new: Soviet Aids propaganda cost countless lives*. [online] Available at: https://www.theguardian.com/science/blog/2017/jun/14/russian-fake-news-is-not-new-soviet-aids-propaganda-cost-countless-lives.

Hutchings, S., Tolz, V. (2021). *Performing disinformation: a muddled history and its consequences | Media@LSE*. [online] Available at: https://blogs.lse.ac.uk/medialse/2021/10/08/performing-disinformation-a-muddled-history-and-its-consequences/.

International Review of the Red Cross. (n.d.). Liar's war: Protecting civilians from disinformation during armed conflict. [online] Available at: https://international-review.icrc.org/articles/protecting-civilians-from-disinformation-during-armed-conflict-914.

J.-B. Jeangène Vilmer, A. Escorcia, M. Guillaume, J. Herrera, Information Manipulation: A Challenge for Our Democracies, report by the Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces, Paris, August 2018

KING, G., PAN, J. and ROBERTS, M.E. (2017). How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument. *American Political Science Review*, 111(3), pp.484–501. doi:10.1017/s0003055417000144.

Lab, D. (2022). *Analysis: How Ukraine has been Nazified in the Chinese information space?* [online] Doublethink Lab. Available at: https://medium.com/doublethinklab/analysis-how-ukraine-has-been-nazified-in-chinese-information-space-81ce236f6a55 [Accessed 2 Aug. 2022].

Legatum Institute. (2015). *Information at War: From China's Three Warfares to NATO's Narratives*. [online] Available at: https://li.com/reports/information-at-war-from-chinas-three-warfares-to-natos-narratives/ [Accessed 2 Aug. 2022].

Lucas, E. and Nimmo, B. "Information Warfare: What Is It and How to Win It," CEPA, November 2015 [Accessed 2 Aug. 2022].

Maizland, L. (2022). *China and Russia: Exploring Ties Between Two Authoritarian Powers*. [online] Council on Foreign Relations. Available at: https://www.cfr.org/backgrounder/china-russia-relationship-xi-putin-taiwan-ukraine.

Maschmeyer, L. (2021). CSS Analyses in Security Policy Digital Disinformation: Evidence from Ukraine. [online] (278). Available at: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse278-EN.pdf.

Mckew, M.K. (2017). *The Gerasimov Doctrine*. [online] POLITICO Magazine. Available at: https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia-foreign-policy-215538/.

MCLC Resource Center. (2016). *Truth of Mao Zedong's Collusion with the Japanese Army (1)*. [online] Available at: https://u.osu.edu/mclc/2016/07/02/truth-of-mao-zedongs-collusion-with-the-japanese-army-1/.

Meister, S. (2016). *The 'Lisa case': Germany as a target of Russian disinformation*. [online] Available at: https://www.nato.int/docu/review/articles/2016/07/25/the-lisa-case-germany-as-a-target-of-russian-disinformation/index.html.

Mesnards, N.G. des, Hunter, D.S., Hjouji, Z. el and Zaman, T. (2020). Detecting Bots and Assessing Their Impact in Social Networks. *arXiv:1810.12398 [physics, stat]*. [online] Available at: https://arxiv.org/abs/1810.12398.

Nikolas K. Gvosdev. (2012). "Chapter 11: The Bear Goes Digital, Russia and Its Cyber Capabilities" In Reveron, Derek S. Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World. Georgetown University Press

OII (2018). *DemTech | Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation*. [online] Available at: https://demtech.oii.ox.ac.uk/research/posts/challenging-truth-and-trust-a-global-inventory-of-organized-social-media-manipulation/ [Accessed 2 Aug. 2022].

P. Charon and J.-B. Jeangène Vilmer, Chinese Influence Operations: A Machiavellian Moment, Report by the Institute for Strategic Research (IRSEM), Paris, Ministry for the Armed Forces, October 2021.

Palmer, J. (n.d.). *Why China Keeps Spinning COVID-19 Conspiracies*. [online] Foreign Policy. Available at: https://foreignpolicy.com/2021/08/11/china-coronavirus-origin-conspiracy-wilson-edwards-fort-detrick/.

Pamment, A.W., James and Pamment, A.W., James (n.d.). *How Do You Define a Problem Like Influence?* [online] Carnegie Endowment for International Peace. Available at: https://carnegieendowment.org/2019/12/30/how-do-you-define-problem-like-influence-pub-80716 [Accessed 2 Aug. 2022].

Pollock, J. (2017). Russian Disinformation Technology. [online] Available at: https://www.technologyreview.com/2017/04/13/152305/russian-disinformation-technology/.

Polyakova, A. (2018). *Weapons of the weak: Russia and AI-driven asymmetric warfare*. [online] Brookings. Available at:

https://www.brookings.edu/research/weapons-of-the-weak-russia-and-ai-driven-asymmetric-warfare/.

Pomerantsev, P. (2015). *How War Changed in 2015*. [online] The Atlantic. Available at: https://www.theatlantic.com/international/archive/2015/12/war-2015-china-russia-isis/422085/.

Posetti, J., Matthews, A. (2018). *A Short Guide to the History of 'Fake News' and Disinformation: A New ICFJ Learning Module*. [online] Available at: https://www.icfj.org/news/short-guide-history-fake-news-and-disinformation-new-icfj-learning-module.

Qiu, L. (2017). Fingerprints of Russian Disinformation: From AIDS to Fake News (Published 2017). *The New York Times*. [online] 12 Dec. Available at: https://www.nytimes.com/2017/12/12/us/politics/russian-disinformation-aids-fake-news.html.

Rosenberger, L. (2020). *China's Coronavirus Information Offensive*. [online] www.foreignaffairs.com. Available at: https://www.foreignaffairs.com/articles/china/2020-04-22/chinas-coronavirus-information-offensive.

Roth, A. (2022). *'It's not rational': Putin's bizarre speech wrecks his once pragmatic image*. [online] Available at: https://www.theguardian.com/world/2022/feb/25/its-not-rational-putins-bizarre-speech-wrecks-his-once-pragmatic-image.

Sazonov, V. and Müür, K. (n.d.). *5. RUSSIAN INFORMATION WARFARE AGAINST UKRAINE I: ONLINE NEWS AND SOCIAL MEDIA ANALYSIS 5.1. Russia's Information Warfare Against Ukraine*. [online] Available at: https://www.ksk.edu.ee/wp-content/uploads/2017/11/RUSSIAN-INFORMATION-WARFARE-AGAINST-UKRAINE-koolon-I-ONLINE-NEWS-AND-SOCIAL-MEDIA-ANALYSIS.pdf.

Seger, E. (2021). *The greatest security threat of the post-truth age*. [online] www.bbc.com. Available at: https://www.bbc.com/future/article/20210209-the-greatest-security-threat-of-the-post-truth-age.

Shambaugh, D. (2007). "China's Propaganda System: Institutions, Processes and Efficacy". China Journal. 57 (57): 25–58. doi:10.1086/tcj.57.20066240. JSTOR 20066240. S2CID 140932475.

Shiwei, C. “History of Three Mobilizations: A Reexamination of the Chinese Biological Warfare Allegations against the United States in the Korean War,” The Journal of American-East Asian Relations 16, no. 3 (2009): 225-226.

Singh, A. (2013). China’s ‘Three Warfares’ and India. *Journal of Defence Studies*, [online] 7(4), pp.27–46. Available at: https://idsa.in/system/files/jds_7_4_AbhijitSingh.pdf.

Smalley, S. (2022). *Network of hyperlocal Russian Telegram channels spew disinformation in occupied Ukraine*. [online] Available at: https://www.cyberscoop.com/network-telegram-russian-disinformation-ukraine-detector-media/ [Accessed 2 Aug. 2022].

Snegovaya, M. (2015). *Institute for the Study of War*. [online] Available at: https://www.understandingwar.org/report/putins-information-warfare-ukraine-soviet-origins-russias-hybrid-warfare [Accessed 2 Aug. 2022].

Solon, O., Dilanian, K. (2020). *China’s influence operations offer glimpse into information warfare’s future*. [online] Available at: https://www.nbcnews.com/business/business-news/china-s-influence-operations-offer-glimpse-future-information-warfare-n1244065.

Soviet Influence Activities: A Report on Active Measures and Propaganda, 1986 -87. (1987). [online] Available at: https://www.globalsecurity.org/intell/library/reports/1987/soviet-influence-activities-1987.pdf.

Venkataramakrishnan, S. (2020). *The real fake news about Covid-19*. [online] Financial Times. Available at: https://www.ft.com/content/e5954181-220b-4de5-886c-ef02ee432260 [Accessed 3 Aug. 2022].

WAHLSTROM, A. et al. (2022). *The IO Offensive: Information Operations Surrounding the Russian Invasion of Ukraine | Mandiant*. [online] Available at: https://www.mandiant.com/resources/information-operations-surrounding-ukraine.

Wardle, C., Derakhshan, H. (2014). *Information disorder: Toward an interdisciplinary framework for research and policy making*. [online] Available at: https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html.

Watts, C. (2021). *Russia's Disinformation Ecosystem - A Snapshot*. [online] clintwatts.substack.com. Available at: https://clintwatts.substack.com/p/russias-disinformation-ecosystem [Accessed 2 Aug. 2022].

web.archive.org. (2019). *习近平引领统战工作进入新时代_原创_中国西藏网*. [online] Available at: https://web.archive.org/web/20190826053157/http:/www.tibet.cn/cn/news/yc/201712/t20171222_5282108.html [Accessed 2 Aug. 2022].

Weedon, J., Nuland, W. and Stamos, A. (2017). *Information Operations and Facebook*. [online] Available at: https://i2.res.24o.it/pdf2010/Editrice/ILSOLE24ORE/ILSOLE24ORE/Online/_Oggetti_Embedded/Documenti/2017/04/28/facebook-and-information-operations-v1.pdf.

Weisburd, A. (2016). *Trolling for Trump: How Russia Is Trying to Destroy Our Democracy*. [online] War on the Rocks. Available at: https://warontherocks.com/2016/11/trolling-for-trump-how-russia-is-trying-to-destroy-our-democracy/.

Whyte, C., Thrall, A., Mazanec, B. Information Warfare in The Age of Cyber Conflict, Routledge (2021), Chapters 2, 11, 12.

Woolley, S. and Howard, P. (2016). Political Communication, Computational Propaganda, and Autonomous Agents Introduction. *International Journal of Communication*, [online] 10, pp.4882–4890. Available at: https://ijoc.org/index.php/ijoc/article/viewFile/6298/1809 [Accessed 27 Oct. 2019].

Young, V. (2020). *Nearly Half of the Twitter Accounts Discussing 'Reopening America' May Be Bots - News - Carnegie Mellon University*. [online] www.cmu.edu. Available at: https://www.cmu.edu/news/stories/archives/2020/may/twitter-bot-campaign.html.